Running head: HIPAA Privacy and Security Standards

HIPAA Privacy and Security Standards: A Gap Analysis for the Compliance Challenge at the Northern Arizona VA Health Care System (NAVAHCS)

Sharon M. Millican

U.S. Army-Baylor University

Graduate Program in Health Care Administration

June 7, 2002

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2002	**Final**	**Jul 2001 - Jul 2002**

4. TITLE AND SUBTITLE
HIPAA Privacy and Security Standards: A Gap Analysis for the Compliance Challenge at the Northern Arizona VA Health Care System (NAVAHCS)

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Sharon M. Millican

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Northern Arizona VA Healthcare System (NAVAHCH) 500 North Highway 89 Prescott, Arizona 86313

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
US Army Medical Department Center and School Bldg 2841 MCCS-HRA (US Army-Baylor Program in HCA) 3151 Scott Road, Suite 1412 Fort Sam Houston, TX 78234-6135

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
38-02

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

There is a difficult and notable challenge facing the healthcare industry in the United States that will profoundly change the way business is conducted. Congress recognized the need for national patient record privacy standards in 1996 when it enacted the Health Insurance Portability and Accountability Act (HIPAA). The law required new safeguards to protect the security and confidentiality of personal health information and mandated implementation within a strict timetable. Industry experts and professionals who have been working on the privacy and proposed security standards say that covered entities need to begin the process of inventorying their organization immediately. The purpose of this project is twofold: (a) to conduct a baseline assessment inventory on the current environment of NAVAHCS policies, processes, and technology with respect to the HIPAA privacy and security standards and (b) to use the information gathered from the baseline assessment to conduct a gap analysis to determine vulnerabilities and enable NAVAHCS to identify necessary process changes and system remediations.

15. SUBJECT TERMS
HIPAA Privacy and Security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**115**	

Acknowledgements

I would like to acknowledge and thank everyone at NAVAHCS who shared their time with me during the months I was researching this project. Although I cannot name them all, everywhere I went I met with colleagues who were very generous and enthusiastic with their observations and insight. In particular I would like to thank Liddy Atkeson, Chief of the Resource Management Service line, Sharon Chapman, Privacy Officer, and Jim Orey, Information Security Officer, for their help. They were never too busy to answer my questions and they provided substantial insight into the compliance challenges ahead.

I would also like to thank my preceptor, Patricia McKlem for sharing her perceptions and suggestions and providing much needed encouragement and support.

Abstract

There is a difficult and notable challenge facing the healthcare industry in the United States that will profoundly change the way business is conducted. Congress recognized the need for national patient record privacy standards in 1996 when it enacted the Health Insurance Portability and Accountability Act (HIPAA). The law required new safeguards to protect the security and confidentiality of personal health information and mandated implementation within a strict timetable. Industry experts and professionals who have been working on the privacy and proposed security standards say that covered entities need to begin the process of inventorying their organization immediately. The purpose of this project is twofold: (a) to conduct a baseline assessment inventory on the current environment of NAVAHCS' policies, processes, and technology with respect to the HIPAA privacy and security standards and (b) to use the information gathered from the baseline assessment to conduct a gap analysis to determine vulnerabilities and enable NAVAHCS to identify necessary process changes and system remediations.

Table of Contents

HIPAA Privacy and Security Standards: A Gap Analysis for the Compliance Challenge at the Northern Arizona VA Health Care System

Introduction

There is a difficult and compelling challenge facing the healthcare industry in the United States. Congress recognized the need for national patient record privacy standards in 1996 when it enacted the Health Insurance Portability and Accountability Act (HIPAA). The law required new safeguards to protect the security and confidentiality of personal health information and mandated implementation within a strict timetable. However, the absence of a comprehensive interpretation of the regulations, along with the broad scope of the requirements and the fact that the final rules have not yet been completely developed, puts an extreme onus on health care providers. It is from these circumstances that this project will attempt to make assessments and develop a plan, which can aid NAVAHCS in addressing those challenges within the framework of the privacy and security regulations.

Problem

HIPAA is rapidly becoming a major issue for the healthcare community. It will have a significant, ongoing impact on healthcare providers as they struggle with compliance. The problem is exacerbated by the short implementation timeline. After the final standards are adopted, healthcare providers must comply within 24 months. Compliance is mandatory and there are significant criminal and civil penalties for non-compliance, as well as serious ethical and business liabilities.

Many hospitals and other healthcare provider organizations have spent years simply waiting for the outcome of the final standards to be known rather than moving ahead to prepare for anticipated changes. Industry experts and professionals who have been working on the privacy and proposed security standards say that executives, managers, and clinicians need to begin the process of inventorying their organizations immediately.

There are no quick ways to institute changes as comprehensive as these. HIPAA has enterprise-wide effects and working through the policies and practices will be an extensive and complex endeavor. There are legal, regulatory, process, security, and technological aspects to each of the proposed rules that must be evaluated before a facility can begin an implementation plan. Information technology (IT) systems and health information management systems (HIMS) will require some degree of retooling, as well as operational and procedural changes. The privacy and security regulations will be the most costly and difficult to implement and maintain, because they are so broad in scope, less well defined, and require constant vigilance for ongoing compliance,

HIPAA is a multifaceted regulation that will involve planning, action, and attention to detail across a wide range of areas, departments, operations and activities. To solve the problem of implementation and compliance, health care providers, including NAVAHCS, must rely on multidisciplinary collaboration to assess where an organization currently stands in relation to the regulations. It is imperative for organizations to begin now because the clock is ticking.

Literature Review

> Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not to be spread abroad, I will keep silence, counting such things to be as sacred secrets. Oath of Hypocrites, 4th Century BCE

The right to privacy is a fundamental privilege and an inherently human expectation. Privacy is a value that in many ways defines our individual and collective freedom. Historically, this nation has placed the rights of the individual at the vanguard of our democracy. Justice Brandeis, in discussing privacy, called it: “the most comprehensive of the rights of man and the right most valued by civilized men” (American Civil Liberties Union, 2001).

Autonomy as an elemental, personal freedom has long been treated as a major value within our society, directing moral analysis primarily toward the individual and his rights of independence, self-reliance, and privacy (Morreim, 1995). Autonomy is a core value in the field of bioethics and an important component of privacy.

Our culture has been transformed in the last two decades by the rapid introduction of astounding new technology into the world of communication. This explosion in communication technology has generated an accelerated and unchecked dissemination of information. People and business organizations have the ability to interact with each other in ways that are faster, more efficient, and more "virtually" realistic than ever before. Our society has incorporated satellite transmissions, videoconferencing, and global cellular services which have allowed us to collect, extract, transport, and use vast quantities of information in totally new ways (Bengani, 1997). Never before has so much personal information been available to be controlled and transmitted electronically.

Personal health information moves throughout hospitals, clinics, private physician's offices, third party payers, and businesses. It moves across county, state, and national boundaries. Private health information is amassed, shared, studied, and warehoused with few legal guidelines or consistent safeguards in place to protect the personal and family secrets of vulnerable individuals. The environment for information is moving rapidly from paper forms and files to a purely electronic medium, which has given organizations an ability to link previously distinct information together and send it through different sources to many destinations (Center For Democracy & Technology, 2000). This has created unique challenges for privacy.

At the beginning of this new millenium, our society faces pivotal questions about

the impact of an increasingly information driven health and business culture. Will the expeditious and unrestricted flow of information make life better? How will it impact our individual freedom? Will the world pay the price in the currency of lost privacy?

Although the public has only recently become aware of the many potential uses for its private health information, interest in confidentiality is burgeoning. Consumer fear over the apparent erosion of personal privacy has led to a response from government agencies addressing the need to protect individual health information.

Donna Shalala, former Secretary, U.S. Department of Health and Human Services stated:

> We are at a decision point. Depending on what we do, revolutions in health care, biotechnology, and communications can hold great promise or great peril. We must ask ourselves: Will we harness these revolutions to improve, not impede health care? Will we strengthen not strain the very lifeblood of our health care system – the bond of trust between a patient and a doctor? When all is said and done, will our health care records be used to heal us or reveal us? (Shalala, 1997, p. 3).

Medical informatics has no doubt streamlined practice management, automated protocols, and facilitated the aggregation of data that have allowed organizations to both utilize and disseminate information rapidly. But, many systems rely on decades old technology that is not robust enough to track information at the level of individual data elements or the individual user. The transition from fee-for-service health care to managed care has led to a demand for an unprecedented depth and breadth of personal information from a variety of healthcare entities (Korpman, 2001).

Modern business culture is predicated on the belief that greater access to information is beneficial to the efficient working of any organization, including the health care industry, but this enhanced functionality can be abused. It is imperative that we ask ourselves <u>who</u> is allowed to see a patient's diagnosis and <u>how</u> is the access

controlled?

Computers, copiers, FAX machines, and E-mail with shared access can all compromise confidentiality by putting sensitive information into the wrong hands. The expanding capabilities of technology and the immense amount of information stored in databases is causing people to lose control of the information they want to keep in their own private domain (Bengani, 1997).

The right to privacy protects liberty by delineating a zone of private life that by its *nature* should be protected. Beauchamp and Childress define privacy as "a state or condition of physical or informational inaccessibility, with control over privacy or a right to control privacy, which involves the agent's right to control access" (Beauchamp & Childress, 1994). They emphasize that the definition of privacy focuses on *powers* and *rights* rather than conditions.

However, some Americans have become so concerned about those very conditions surrounding electronic record keeping that they withhold information from their doctors in an effort to prevent the creation of a medical record and a potentially discriminatory information trail (Goldman, 2000). They fear that disclosure of compromising medical records may result in loss of employment or denial of insurance. This perceived lack of privacy can potentially diminish the access to and quality of health care when people feel that they are forced to make a choice between their privacy and receiving health care (Health Privacy Project - Institute for Health Care Research and Policy, 2000). Secretary Shalala in describing a proposal to protect patients' personal medical records stated:

> We cannot allow the absence of privacy protections to compromise the quality of care in our nation. Our proposals will provide Americans with greater peace of mind as they seek care, yet they are balanced with the

> need to protect public health, conduct medical research and improve the quality of health care for the nation. (HHS News, 1999, p. 1)

The protection of health information to date has not been completely neglected, although it has been primarily the purview of the states to enact legislation that safeguards personal data. While every state has enacted laws to protect privacy of personal information, the laws lack standardization and completeness (Office of the Assistant Secretary for Planning and Evaluation, DHHS, 2000). Many state laws, although protecting health information that relates to stigmatized conditions, (HIV, communicable diseases, mental illness, etc.) do not extend comprehensive protections to ordinary medical records. Many fail to provide such basic protection as securing a patient's legal right to see a copy of his own medical record (Institute for Health Care Research and Policy, Georgetown University, 1999). Effective federal rules do not exist which set national standards and practices, providing baseline ground rules for health plans, covered entities, and health care providers. There is a need to erect a "federal floor of safeguards" to protect the confidentiality of private health information (Office For Civil Rights, 2001). Decades of a hodge-podge of privacy enhancing statutes have not provided a comprehensive piece of legislation including such key provisions as access, limits on disclosure, requirements regarding employer notification, use in research, and penalties that will apply to all health care providers, plans, and clearinghouses. An abbreviated list of regulations passed at the federal level over the last 35 years to enact safeguards in a variety of fields includes:

- Freedom of Information Act (1966, amended 1974, 1976)
- Fair credit Reporting Act (1970)
- Privacy Act (1974)
- Family Educational Rights and Privacy Act (1974)
- Right to Financial Privacy Act (1978)
- Electronic Communications Privacy Act (1986)

- Computer Security Act (1987
- Privacy Protection Act (1988)
- Video Protection Act (1988)
- Telephone Consumer Protection act (1991)
- Telecommunications Act (1996)
- Health Insurance Portability and Accountability Act (1996)
- Balanced Budget Act (1997)
- Consumer Bill of Rights and Responsibilities (1997)
- Identity Theft and Assumption Deterrence Act (1998)

(eRiskSecurity, 2001)

In 1996, Congress recognized the need to protect patient privacy through national legislation. Legal control of health information was primarily restricted to state law, which varied greatly in scope and strength. Shalala (1997) described it as “a morass of erratic law, both statutory and judicial, defining the confidentiality of heath information.” Congress set a deadline for itself, as part of the Health Insurance Portability and Accountability Act (HIPAA), to issue regulations and enact comprehensive national protections on medical record privacy. When Congress failed to pass a privacy statute or define legislative standards by this deadline, HIPAA required that the Department of Health and Human Services (HHS) issue regulations (Health Privacy Project, 2000).

As required, HHS consulted with the National Committee on Vital and Health Statistics (NCVHS) and the Attorney General to develop the recommendations. In addition to all required consultations, HHS also requested the participation of representatives from the Departments of Justice, Commerce, Defense, Veterans Affairs, and Labor, and the Offices of Management and Budget, Personnel Management, and the Social Security Administration (Office of the Assistant Secretary for Planning and Evaluation, 2000).

On November 3, 1999 HHS published a Notice of Proposed Rule Making (NPRM) for “Standards for Privacy of Individually Identifiable Health Information” (45 C.F.R.

Parts 160-164). This notice established regulations to protect the privacy of individually identifiable health information maintained or transmitted electronically by health care providers, hospitals, health plans, health insurance providers, and health care clearinghouses (Joint Healthcare Information Technology Alliance, 2000).

The use of these regulations is designed to provide new rights for individuals and improve the efficiency and effectiveness of public and private health programs by defining and limiting the circumstances in which an individual's health information may be used or disclosed. The intent is to reduce healthcare fraud and abuse, guarantee security and privacy of health information, and impose penalties for enforcement (Putt, 2000).

The regulations are founded on five key ideas:

- Consumer Control: Controls disclosures and rights to access including consent and authorization. Legislation to strengthen the ability of consumers to understand and control what happens to their health care information.
- Boundaries: The limits of coverage and who is covered. Health care information should be used only for health purposes, treatment and payment. Legislation imposes a legal duty of confidentiality on those who provide and pay for health care.
- Accountability: Specific federal penalties and legal recourse through sanctions and new avenues of redress if an individual's right to privacy is violated.
- Public Responsibility: Reflects the importance of balancing privacy protections with the public responsibility to support and protect public health, medical research, and the improvement of quality of care through the use and disclosure of information for health oversight activities.
- Security: Responsibility to protect health information against deliberate or

inadvertent misuse or disclosure. This includes administrative procedures, physical safeguards, and technical security services and mechanisms (Beacon Partners 2000; see also Shalala, 1997).

HIPAA specifies regulations for the standardization of electronic transactions (administrative and financial); medical data code sets; unique health identifiers for patients, providers, health plans and employers; claims attachments that support requests for payment; electronic signatures; data security, and enforcement. When the proposed framework for the regulation was initially developed, HHS included only health data that had been stored or transmitted electronically, but the final rule extended privacy protection to personal health information in whatever form it is preserved or exchanged including electronic, written, and oral. Together these standards are intended to smooth the flow of information integral to healthcare operations while protecting confidential information from inappropriate access, disclosure, and use (Health Privacy Regulations, 2001).

Only two of the proposed rules have been published in final form. The Final Rule on Security Standards has not been published in the Federal Register, but is expected to be published by the end of the year. The transaction and code set regulations have just had their compliance date delayed one year by Public Law 107-105 (formerly HR 3323) signed by President Bush and enacted December 27, 2001 (American Hospital Association, 2001). The Privacy Rule became effective on April 14, 2001. Most health plans and providers that are covered by the rule must be in compliance with the requirements no later than two years from that date. The law does not give HHS the authority to regulate other types of private businesses or public agencies such as life insurance companies, employers, or public agencies that dispense welfare benefits or

social security. HHS continues to review input received during the public comment period and states that it can and will issue proposed modifications at any time. These modifications are intended to correct newly recognized problems that may negatively impact on consumers' access to care or the quality of their healthcare (U.S. Department of Health and Human Services Office for Civil Rights, 2001).

HHS reviewed and considered more than 50,000 public comments about the rule before publishing final standards in December of 2000 (HHS News, 2001). Secretary Tommy G. Thompson (U.S. Department of Health and Human Services) again requested feedback and commentary on the rule before allowing it to take effect on April 14, 2001 (Braithwaite, 2001). During the interim, HHS met with a diverse collection of lawmakers, interest groups, health care leaders, and private citizens, as well as considering more than 24,000 written comments. Secretary Thompson stated that President Bush:

> considers this a tremendous victory for American consumers, who will continue to receive high-quality health care without sacrificing the confidentiality of their private health matters. The President believes this patient privacy rule will deliver strong and long overdue protections for personal medical information while maintaining the high quality of care we expect in this great nation. Our citizens will finally have the peace of mind of knowing their health records are safe and protected (Thompson, 2001).

What has become known as the final rule establishes the privacy safeguard standards that covered entities must meet, but it also provides them the necessary flexibility to design their own policies and procedures in accordance with the nature of the facility's business, size, and resources. The HHS Office for Civil Rights (OCR) will enforce the final rule but will also provide assistance to providers, plans, and clearinghouses to comply with the requirements of the regulation (HHS Fact Sheet, 2001).

The implementation of HIPAA regulations carries consequences, which are both positive and negative, and the anticipation of these consequences is a source of legitimate anxiety to those affected. A survey of the stakeholders involved presents a divided outlook.

Many powerful organizations, disturbed about the expected arduous effort required to redesign workflow, have protested the implementation of the HIPAA regulations and the proposed consequences for lack of compliance. Others have hailed it as the most "sweeping legislation to impact the healthcare industry in more than 30 years" (Harrington, 2001).

There is now a compelling business reason for the industry to clear the way to less complicated administrative transactions. Without this mandate from HHS, many more years could have elapsed without standardizing the security and privacy infrastructure. The opportunity to create a uniform format for eligibility, payments, and claims, translates into one claim format, one remittance format, and one eligibility inquiry for both providers and payers.

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) favors the regulations as long as access to crucial clinical information is not limited. It will be assessing the implications of the HIPAA standards on its own accreditation process to determine if changes are necessary. Currently its standards for healthcare organizations require that the confidentiality, security, and integrity of all data and medical information be maintained (Noble, 2001). Still, some JCAHO representatives have noted that they might have to enter into contracts with each of the 18,000 facilities that JCAHO surveys in order to comply with the business associate arrangement. Anthony Tirone, JCAHO director of federal relations, Washington, DC stated that

comments were submitted to HHS Secretary Thomson on the issue of an accreditor being considered a business associate under the regulations, rather than a health care oversight agency. In preparation, JCAHO is developing a standard agreement that will delineate its use and protection of protected information shared with each accredited organization (Tirone, 2001).

What are the consequences of such uniformity and regulation? It is projected that organizations will experience a reduction in manual processing and a decrease in the variability of processes. The customer service benefits are expected to include reduced processing errors, a shortened claims processing cycle, and more online claims status reporting, all resulting in reduced waiting times for verification of eligibility. It is anticipated that standardization will assist providers in coordinating referrals more expeditiously (Cassidy, 2000a).

The outcome could be an untapped source for administrative cost savings and workflow efficiency through an industry-wide operational analysis and re-engineering. The Centers for Medicare and Medicaid Services (CMS), formerly HCFA, estimates that health plans and providers will share in $29.9 billion cost savings over the next 10 years. The Boundary Information Group of Denver, CO, is estimating that medical groups may achieve 51% savings in their business operations, 12% in the provision of managed care, and 37% in bad debt, postage, and other administrative costs (Harrington, 2001). A facility with a single integrated system will have a much simplified task. Costs per transaction can expect to be trimmed, as the organization is better able to aggregate information that will now be standardized. Information services that currently serve multiple practices will be in a position to capture statistically significant data extracted from the flow of business transactions and to make meaningful

comparisons across a whole range of payers. Some see this as an opportunity that has been enhanced by HIPAA constraints to make money to pay for HIPAA burdens (Nolin, 2001).

Effective, secure, and reliable information technology systems can deliver substantial cost savings while providing timely, accurate, and secure access to vital medical information. Worldwide growth in the IT industry, with its unprecedented advances in processing power and transmission speed, has the potential to increase productivity and improve the quality of healthcare services. New technologies most certainly will dramatically alter the way the business of healthcare is currently administered, as long as computer systems and networks can preserve the confidentiality of the patient's medical record (Kammer, 2000).

The challenge extends far beyond averting a medical-legal quagmire. Healthcare providers can use HIPAA to make improvements to the very business of providing healthcare. Risk managers can expect to benefit by security guidelines, and patients will profit by the attention to privacy and from the possible reduction in cost if the hoped for system-wide efficiencies result.

While complying with HIPPA regulations will require a significant investment of time and money, it also represents an opportunity for health plans to seize the initiative and transform healthcare. These changes, although mandated, may provide solutions that will help the industry to realize the highest objective of managed care: to make the provision of healthcare more efficient and more responsive to patients. These are strong arguments in support of the HIPAA transition.

However, the perceived benefits of HIPAA implementation must be approached with a degree of caution. Experience has shown that compliance with mandatory

regulations often results in unforeseen and unavoidable costs and burdens. This fact has not been lost on the industry, and many organizations and agencies have voiced concerns.

Although intended to reassure consumers of the confidentiality of their personal health information while broadening the scope of privacy protection, HIPAA seems like a tidal wave hitting the healthcare industry and immersing organizations in a sea of details, questions, and uncertainties. Deciphering and working though the comprehensive polices and practices has turned out to be a complex and multifaceted process that engenders apprehension. Preparation for HIPAA has been likened to preparation for Y2K, although it will require a much more interdisciplinary approach to assess risk points in the physical and technical information flow of an organization. Covered entities will have to deal with considerable training and education for staff and will also have to work with vendors and business partners in reviewing contracts for compliance (Hagland, 2001).

In testimony submitted to congressional committees and federal agencies in 2001, the American Hospital Association (AHA) addressed the patient care and operational issues raised by the consent provision in the final rule on medical privacy. The unintended consequence of requiring written consent prior to the first contact between patient and provider can be a serious disruption in patient care and essential hospital operations.

As currently written, the privacy rule will prevent a hospital from using any information about a patient to schedule inpatient or outpatient procedures until the patient receives the hospital's privacy notice and returns a signed consent form. Under the regulation, the privacy notice will be over 10 pages even before the addition of the

provisions required by state law. In order to simply schedule hospital care, patients must obtain the privacy notice and a separate consent form, read both documents and sign and return the consent to the hospital.

Many strategic working groups are recommending that patients be required to sign a new written consent form each time they present for care based on the perceived risks associated with relying on prior consent and the administrative difficulty and cost associated with tracking them (Presentation by the AHA, 2001).

Hospitals will also need to conduct a comprehensive audit of all created and stored “protected health information” (PHI), change their computer systems to limit access to information, provide staff training, and conduct ongoing, expensive compliance audits. Many covered entities will need to invest in new information systems or upgrade what they currently have in place, and it is estimated that this could cost many billions of dollars.

Hospitals will have to identify all business partners who use or access their PHI. According to the regulation, covered entities must hold their partners accountable with a written contract and, depending upon the number of business associates, monitoring compliance can be an enormously burdensome proposition (Mitchell, 2000). First Consulting Group (FCG), a multinational pharmaceutical/life sciences and health information technology services firm has estimated that the overall cost for achieving compliance could be as much as $22.5 billion dollars over five years, with ongoing costs expected to exceed $500 million a year. First Consulting Group also states that HHS’ cost estimates lack a “stated or logical source” and “grossly underestimate” the costs of the technical requirements (Mitchell, 2000).

A letter sent to President Bush from Bill Thomas, Chairman of the US House of

Representatives Ways and Means Committee, and Nancy Johnson, Chairman of the Health Subcommittee described similar concerns. They acknowledged that it is "critical" to balance patient rights against "legitimate health care needs". They cite the requirement to obtain written consent for standard uses of information, restrictions on the amount of medical information that can be shared among providers, the need for advisory opinions to identify conflicting state law, and the paperwork created by business partner contracts as unduly burdensome (Davidson, 2001).

The Association of American Physicians and Surgeons filed a lawsuit against HHS on August 30, 2001 alleging that the agency's privacy regulations infringe on physician-patient rights by adversely affecting communications. An earlier suit filed this year by the South Carolina Medical Association, the Louisiana State Medical Society, and others focuses on the legality of the HIPAA law itself (Health Information Compliance Alert, 2001).

The House of Representatives Committee on Appropriations recommended in a report to the full House in October of 2001, that the Secretary HHS evaluate the effects of the substantial investment and monetary expenditures that health care organizations will be required to make. Furthermore, the Committee directed the Secretary to identify and report to it any sources of federal funding that might be available to help defray the costs of complying with HIPAA requirements (Departments of Labor, Health and Human Services, and Education, 2002).

The American Medical Association has significant questions about the cost and disruption of HIPAA compliance and fears that it may pose daunting administrative burdens for medical practices over the next two years. Only 27% of health care organizations have begun preliminary budgeting for HIPAA compliance activities

(American Medical Association, 2001).

The American Hospital Association (AHA) has also provided notable input to HHS on issues such as data aggregation for benchmarking, requirements for business associates, disclosures to the government, and other concerns relating to oral communication and consent (American Hospital Association, 2001). The AHA believes that the medical privacy rule in its present form may be unworkable. Melinda Hatton, Chief Washington Counsel of the AHA, states that the AHA will ask Congress for federal funds to help hospitals comply with regulations that it considers “unnecessarily complex and burdensome” (Noble, 2001).

The Blue Cross/Blue Shield Association, the Medical Group Management Association, and the Workgroup for Electronic Data Interchange joined the AHA during a nationwide Internet broadcast by the Journal of Health Care Finance to pose questions about the risk of installing expensive security systems. Specifically, these groups called attention to concerns about installing systems that will later need to be changed, the overall cost of compliance, and the differing timetables on actualizing the distinct rules. (Noble, 2001).

The American Association of Health Plans has also expressed concern about the scope of consent relative to its ability to obtain the patient data necessary to conduct health care operations. It fears that providers’ consent forms will be too narrowly interpreted to allow for adequate data sharing (Health Privacy Regulation, 2001).

The American Pharmaceutical Association questions how the consent requirement may be applied and if pharmacies must obtain written consent prior to filling a prescription for the first time. The American Health Information Management Association (AHIMA) has correlated this timing issue to what hospitals face with respect

to getting background medical information from patients before admission (Health Privacy Regulation, 2001).

The regulation regarding the protection of patients' privacy extends to contractual arrangements with each covered entity's business associates, attorneys, auditors, accountants, data processing firms, and others. Many provider groups are concerned about safeguarding the confidentiality of protected health information through the establishment of contractual assurances of mutual compliance (Health Privacy Regulation, 2001).

The resulting effects of HIPAA implementation will only be known after compliance has been initiated. Unfortunately, it is not possible to stand back and adopt a "wait and see" attitude. Action must be taken now, and a determination of current status is an important and appropriate first step.

Purpose of the Study

The purpose of this project is to conduct a baseline assessment inventory on the current environment of NAVAHCS' policies, processes, and technology with respect to the HIPAA privacy and security standards. The information gathered from the baseline assessment will then be used to conduct a gap analysis, or a comparison of the current environment against the regulatory requirements. This study will focus on NAVAHCS' current state of readiness as of March 2002 relative to the mandated changes.

The HIPAA standards constitute enterprise-wide issues and are not limited simply to information technology. There are legal, regulatory, policy, security, and technological aspects to each of the proposed rules and each must be evaluated before an institution can begin its implementation plan. The intent of this inquiry is to proactively identify the scope of specific projects necessary for compliance with the

standards.

Technology has provoked a system wide renegotiation of the contract between the individual and his healthcare system over the use of personal information. Because of the complexity of the HIPAA privacy regulations, and because they will significantly impact the way organizations conduct their businesses, now is the time to determine what will be needed to be in full compliance.

The following questions provide the basis for the supporting objectives of this examination.

- What does NAVAHCS have to do to be in compliance?
- Will technical changes need to be made to NAVAHCS' systems?
- Which policies will need to be reviewed, revised or developed?
- What internal processes in HIMS, IS, patient care, and clinical care support will need to be altered?
- Which staff members will be affected?
- What skills do staff members need to develop?
- What educational process for staff and new employee orientation needs to be developed?
- What are the greatest opportunities for improvement in HIPAA related areas?

Answers to these questions should reduce the processing and transition time as well as administrative expenses, by providing NAVAHCS with the opportunity to streamline its primary method of PHI. The ability to proactively reengineer business practices, and change business methods and organizational culture will be essential determinants of successful compliance.

Organizing a compliance program to conform with regulations this diverse and

comprehensive requires a systematic approach and deliberate action. Safeguarding privacy and improving health care need not be diametrically opposed. The key values of privacy, access, and quality are linked.

It will be vitally important to incorporate cultural change in order to inspire an organizational vision of a hospital that is known for respecting and protecting the confidentiality and security of its patients' private, health information. Now is the time to prepare, educate, and respond to our consumers and stakeholders and to make the transition to new practices.

Method and Procedures

Understanding the Regulations, Assessing the Practice, and Closing the Gaps:

The researcher will perform a risk assessment to compare current business practices with the new HIPAA directives. From this, an action plan will be developed from the identified and prioritized findings in order to progress towards compliance. For the purposes of this proposed project, the assessment will be limited to those components of the regulation that relate specifically to privacy and security of personal health information.

Procedure for the Gap Analysis/Risk Assessment for NAVAHCS:

- Identify primary areas for review within the framework of the HIPAA privacy and security requirements.
- Examine the internal and external flow of personal health information.
- Inventory protected health information in order to understand where and how information is received, how it is used, stored, disclosed, and disposed of, paying close attention to:
    - clinical care lab, prosthetics, pharmacy, and other ancillary areas

where data are used and disclosed.

  - administrative transactions, i.e. billing, insurance, patient registration, eligibility, appointments, etc.
  - financial transactions/resource management
  - volunteer service organizations
  - quality programs

- Identify relationships with other covered entities.
- Identify relationships with business associates.
- Compile all information privacy and security policies currently in place and evaluate against regulatory mandates.
- Develop qualitative measurement criteria as a tool to evaluate the current environment for each of the standards in order to identify readiness gaps and potential vulnerabilities.
- Determine the areas that present the greatest potential compliance risk.
- Establish priorities to guide the development and implementation of a HIPAA privacy and security compliance plan in the future.

(Apple & Brandt, 2001).

Format: Assessment questions for conducting the gap analysis will follow a brief explanatory description of the standards in the Privacy and Security subsections of the rule. These questions will form the basis of a survey for each department within NAVAHCS.

Measurement criteria used in this research will be a ranking of current readiness weighed against the HIPPA requirements as suggested by the VHA Office of Information (OI) HIPAA Workgroup. The OI ranking criteria will be used in order to

provide consistency with VHA methodology and the OI Workgroups.

Ranking Scale:

0 – No identified process or control
1 – Informal or partial process or control
2 – Process or controls implemented for many required HIPAA elements
3 – Process or controls fully implemented for all required HIPAA elements.
4 – Process or controls exceed required HIPAA elements
(VHA Office of Information, 2000).

Standards for Privacy of Individually Identifiable Health Information

(45 CFR Parts 160 and 164)

The HHS Final Rule for Standards on the Privacy of Individually Identifiable Health Information is part of HIPAA's administrative simplification provisions (as are the Security standards). These standards provide guidelines to protect the privacy of health information while also ensuring its availability for care. They also aim to improve the overall efficiency and effectiveness of the healthcare system (Amatayakul, 2000). The standards address the use and disclosure of protected health information; consent requirements; business associates; authorization requirements; individuals' rights; and the "*minimum necessary*" requirement.

The rules limit the use and release of private health information unless consent or authorization is obtained, but they do not prescribe the particular measures that covered entities must take to meet the standards. They give patients new rights to access, copy, and amend their medical records and to receive an accounting of who else has accessed them. The final rule restricts most disclosures to only the minimum amount of protected information necessary for the intended purpose and requires that facilities develop and use contracts that will ensure that business partners also protect that privacy. Finally, HIPAA establishes criminal and civil monetary penalties against those

covered entities that fail to comply and improperly use or disclose protected patient information (Office For Civil Rights, 2001). As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct financial and administrative transactions. These will be referred to as covered entities throughout the rest of the paper (BENEFITS next, 2001).

Use and Disclosure of Protected Health Information for Treatment, Payment, and Health Care Operations §164.502(a)

The rule states that "when using or disclosing protected health information (PHI) or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the *minimum necessary* to accomplish the intended purpose of the use, disclosure, or request" [65FR82805 & 65FR82819].

A covered entity is required to disclose information to the individual who is the subject of the information when a proper request for access is made and when required by the Secretary of HHS to investigate or determine a covered entity's compliance with the regulations. Under the HIPAA regulations, use occurs when private health information is shared, employed, applied, utilized, examined, or analyzed within the facility that stores the information. A disclosure occurs when it is transferred, utilized, or divulged in any other manner outside the facility maintaining the information (Bricker & Eckler, 2001).

Covered health information includes any information, oral or recorded in any form or medium, including demographic information that relates to the physical or mental health, or condition of a patient. HIPAA's intent is to recommend a meaningful minimum standard of protection while recognizing that reasonableness may depend on the judgment of each separate facility (Secretary of Health and Human Services, 1997).

The minimum necessary provisions do not apply to:

- Disclosures to, or requests by, a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an authorization requested by the individual.
- Uses and disclosures required by HHS for enforcement or as required by other law (Office for Civil Rights, p.11, 2001).

Non-routine disclosures should be reviewed on an individual basis, and facilities must develop reasonable criteria for determining, and limiting disclosure to only the minimum amount of information necessary to accomplish the purpose.

The Office for Civil Rights, within the U.S. Department of Health and Human Services emphasizes that the purpose of the minimum necessary standard is to make covered entities evaluate their practices and limit unnecessary sharing but not to hinder the use of medical information in legitimate treatment settings, given the job responsibilities of the workforce and the nature of their business. It is expected that policies developed will reflect professional judgment and standards and that the input of professional staff will be utilized so that appropriate care will not be compromised (Office For Civil Rights, 2001).

The rule requires covered entities to designate a privacy official who is responsible for the development and implementation of the policies and procedures and who is responsible for receiving complaints (§164.530).

Assessment Plan:

- Compare current procedures for the use and disclosure of health information with the proposed privacy standards.

- Is there a designated privacy officer for NAVAHCS?
- Does NAVAHCS have a plan in place to provide training to each member of the workforce on the policies and procedures with respect to protected health information (PHI)? §164.530(b)
- Does NAVAHCS account for all disclosures of protected health information for purposes other than treatment, payment, or healthcare operations?
- Are appropriate administrative, technical, and physical safeguards in place to protect the privacy of PHI? §164.530(c)
- Are there policies in place that set reasonable limitations on access to and use of PHI according to professional role and job description?
- Is there a mechanism for employees to complain about possible violations of privacy? §164.530(d)
- Does NAVAHCS provide patients with a *Notice of Privacy Practices* of the uses and disclosures of PHI that it is permitted to make for treatment, payment, and health care operations? §164.520
- Does this notice include a statement about written authorization, consent, and the conditions under which a patient can revoke authorization?
- Does this include those uses for which NAVAHCS does <u>not</u> require the patients written consent or authorization?
- Does NAVAHCS have a mechanism to account for all disclosures of PHI for purposes other than treatment, payment, and healthcare operations (TPO)?
- Does NAVAHCS have sanctions in place against employees who fail to comply with the privacy policies or the requirements of the rule? §164.530(e)
- Is there a process in place for individuals to complain to NAVAHCS about perceived

violations of privacy rights? (Joint Healthcare Information Technology Alliance, 2000; Taylor, 2001).

Consent: 45 CFR §164.506

A covered health care provider must obtain the individual's consent in accordance with the rule prior to using or disclosing PHI to carry out treatment, payment, or health care operations (TPO). Consent grants general permission to use or disclose PHI for multiple visits and different medical conditions. During an emergency situation, uses and disclosure may be permitted without prior consent. If a patient refuses to consent to the use or disclosure of their PHI to carry out TPO, the health care provider may refuse to treat the patient. Patients may revoke their consent in writing and may request restrictions on uses or disclosures of their health information. The covered entity does not have to agree to the requested restriction, but is bound to the extent that it has taken action or agreed. Individuals must be given a notice of the facilities privacy practices and may review it before signing the consent. It will not be necessary for the facility to obtain a new consent annually (Bricker & Eckler, 2001; Health Information Compliance Insider: A Plain-English Guide, 2001; Office For Civil Rights, 2001).

Assessment Plan:

- Does NAVAHCS have a document for required consent for uses and disclosures that is separate from the Notice of Privacy Practices? §164.506(b)
- Is the document written in "plain language" and does it:
    - Inform the individual that PHI may be used and disclosed to carry out TPO?
    - Refer the patient to NAVAHCS' privacy notice and state the patient's rights to review it?
    - State that the patient has the right to request that NAVAHCS restrict how his PHI is used or disclosed to carry out TPO?
    - State that the patient has the right to revoke consent in writing except

to the extent that the facility has taken action?
- State that the patient has the right to inspect and copy information and to seek amendments?
- Describe the procedures for the exercise of rights, complaints, redress, or appeal?
- State that NAVAHCS has reserved the right to change its privacy practices and the terms of its notice, and describe how the patient may obtain a revised notice?

(AHIMA Policy and Government Relations Team, 2001a)

- Does the Notice of Privacy Practices describe how NAVAHCS uses PHI, its legal duties under the regulations, and the individual patient's rights under the regulations?
- Does HIMS have a plan in place to retain signed consent copies for six years from the date of its creation or when it was last in effect?
- If a patient makes a change to his records, does NAVAHCS have a plan in place to inform others who have received the incorrect information about the change?

(AHIMA Policy and Government Relations Team, 2001a; Secretary of Health and Human Services, 1997).

Authorization: §164.508

Authorization is required for any use or disclosure of PHI outside of the context of TPO, and includes training programs and marketing/fundraising materials that identify patients. Treatment cannot be conditional upon obtaining an authorization. An authorization can be revoked at any time, provided that the revocation is in writing. The core elements of patient authorization include:

- A specific, meaningful description of the information to be used/disclosed.
- The name or other identification of the authorizing patient.
- The name or other identification of the recipients of the information.
- The expiration date of the authorization.
- A statement of the patient's right to revoke in writing, and an explanation of how to do so.

- A statement that the recipients may further disclose the information and, in such a case, the information will lose its HIPAA privacy protection.
- A signature of patient/date.
- A description of representative if patient cannot sign the authorization.

(Bricker & Eckler, 2001).

A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes except to carry out TPO. The covered entity may use the notes in training programs in which students, trainees, or practitioners in mental health learn under supervision to improve their skills in individual, family, or group therapy. It may use the notes to defend a legal action or other proceeding brought by the individual.

No patient consent, authorization, or opportunity to object is needed when use and disclosure is required by law, judicial and administrative proceedings, law enforcement requests or health oversight activities. They are not required for organ and tissue donation, emergencies, worker's compensation, or when providing deceased person information to coroners, medical examiners, and funeral directors (Bricker & Eckler, 2001; Taylor, 2001).

The regulation extends the reach of the "Common Rule" as implemented by the Federal Policy for the Protection of Human Subjects (38 CFR Part 16) by requiring that the disclosure of PHI without an individual's authorization for research should be approved by an Institutional Review Board (Joint Healthcare Information Technology Alliance, 2000a).

Assessment Plan:

- Does NAVAHCS have an authorization form written in "plain language" that states that treatment, payment, enrollment in the health plan, or eligibility for benefits is not conditional on the individual's providing authorization for the requested use or

disclosure?

- Does it meet all the “core elements and requirements” as described above?
- Does it have a description of each purpose of the requested use or disclosure?
- Does it contain a statement that the individual may inspect or copy the PHI to be used or disclosed and a description of the right to refuse to sign the authorization?
- Does it clearly stipulate if use or disclosure of the requested information will result in payment to NAVAHCS from a third party?
- If NAVAHCS requests authorization from another covered entity to carry out TPO, does the authorization meet the requirements of the “core elements”, and does it also contain:
    - A description of each purpose of the requested disclosure?
    - A statement that NAVAHCS will not condition TPO, enrollment or eligibility for benefits on the individual providing authorization for the requested use or disclosure?
    - A statement that the individual may refuse to sign the authorization?

(American Health Information Management Association (AHIMA) Policy and Government Relations Team, 2001a; Bricker & Eckler, 2001; Joint Healthcare Information Technology Alliance (JHITA), 2000).

Right of Access and Amendment: (§164.524 and §164.526)

Patients have the right to access their own health information, including the right to inspect and obtain a copy of the information in a designated record set. They have the right to request an amendment or correction of PHI that is inaccurate or incomplete, and they have the right to receive an accounting (audit trail) when PHI has been disclosed for purposes other than TPO. Facilities must respond to request for copies within 30 days and may deny these requests when:

- it could endanger the patient’s life or safety,
- if the PHI makes reference to another person,
- if the request is made by a personal representative and a licensed health care

professional has determined that providing access is likely to cause harm to the individual or another person.

Patients may request review of a denial, and the facility must designate a healthcare professional not involved in the patient's care to conduct the review (AHIMA Policy and Government Relations Team, 2001a; Taylor, 2001).

There are also unreviewable grounds for denial of access. These are:

- If the PHI is maintained in psychotherapy notes.
- If information is compiled in anticipation of, or for use in a civil, criminal, or administrative action or proceeding.
- If the PHI is contained in records that are subject to the Privacy Act 5 U.S.C. 552a, and if denial of access under the Privacy Act would meet the requirements of that law.
- If the individual has agreed to temporary denial of access when consenting to participate in research that includes treatment, and the research in not completed.
- If the PHI was obtained from someone other than a health care provider under a promise of confidentiality, and access would reveal the source of the information (Hughes, 2001).

If the covered entity denies the request, it must provide the individual with a timely written denial in plain language, explaining the basis of the denial and a description of how the individual may complain to the facility.

An individual also has the right to request an *amendment* to his health information. Covered entities may require patients to make any request for amendment in writing and to provide a reason supporting that request, provided that it informs them in advance (§164.526). Action on the request must be taken no later than 60 days after receipt of the request, whether the amendment is granted in whole or in part or denied in whole or in part. Health care organizations may deny the request if the information that is the subject of the request was not created by the covered entity, or is not part of the individuals health record. They may deny the request if it would not be accessible for the reasons described in the *access* section, or if the information is deemed accurate

and complete.

The facility must provide all denials in writing, using plain language and delivering them in a timely manner (60 days or less). The denial must contain the basis for denying the requested amendment and must include a statement of the patient's right to submit a written statement disagreeing with the denial. If the individual chooses not to submit a statement of disagreement, he may still request that his request for amendment and the denial be included with any future disclosures of the PHI that is the subject of the amendment. The facility must also permit the patient to submit a written statement of disagreement with the denial, and then may prepare a written rebuttal to the individual's statement of disagreement.

The patient must be provided a copy of this rebuttal. For purposes of accurate documentation and record keeping, the facility must identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment. The facility must include the statement of disagreement and the material appended along with an accurate summary of the information in any future disclosure. The covered entity that is informed of an amendment to an individual's PHI must amend the material as well (AHIMA Policy and Government Relations Team, 2001a; Bricker & Eckler, 2001; Hughes, 2001).

Assessment Plan:

- Does NAVAHCS have a policy that designates which record sets are subject to access by individuals?
- Does NAVAHCS have a procedure in place to permit individuals to request access to inspect or to obtain a copy of their PHI?
- Does the policy document the title of the persons or offices responsible for receiving

and processing requests for access? Processing responses to a review of denial?

- Is NAVAHCS prepared to respond to requests for PHI that do not require consent, e.g., public health, health oversight, and judicial activities?
- Is there a procedure in place for verifying the identity and authority of persons requesting such disclosures?
- Is NAVAHCS staff informed as to when it is appropriate to deny a request for access?
- Is there a procedure in place to provide written denial?
- Does NAVAHCS have a process to create and provide an audit trail for patients when PHI has been disclosed for purposes other than TPO?

Uses and Disclosures for Public Health Activities:

There are specific instances where dissemination of PHI to a public agency or an individual is necessary. A covered entity may disclose PHI to a public health authority that is legally authorized to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability. PHI may also be disclosed to a person subject to the jurisdiction of the Food and Drug Administration to report adverse events, to track products, or to enable product recalls, repairs, or replacements. If the covered entity or public health authority is authorized by law to notify a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, it may disclose PHI exclusively for public health activities (AAMC - Association of American Medical Colleges, 2001a).

Disclosures about victims of abuse, neglect, or domestic violence §164.5129c):

A covered entity is also permitted, in specified situations, to disclose protected health information about victims of abuse, neglect, or domestic violence without the

patient's consent or authorization. The covered entity may use or disclose PHI only to the extent that it is required by law. The information may be disclosed to a government authority, including a social or protective service agency that is authorized by law to receive such reports. A facility does not need to first obtain consent or authorization when it believes, according to its professional judgement that the disclosure is necessary to prevent harm to the patient. In situations where the facility makes disclosures according to the rule, it must also promptly inform the individual that the disclosure has been made, unless informing the patient would place him at risk of serious harm (AHIMA Policy and Government Relations Team, 2001a).

Assessment Plan:

- Does NAVAHCS have a policy in place for complex permitted reporting requirements for suspected abuse, neglect, or other public health activities?
- Who determines if a reportable event has occurred?
- Who makes the formal report?
- Who makes the decision to report or not to report?
- Is there a process in place for informing the individual about public health reports?
- Does NAVAHCS document when a public health report is made or that a decision was made not to report? (AAMC - Association of American Medical Colleges, 2001).

Business Associate Agreements: [45 CFR §§160.103,164.502(e), 164.514(e)]

The Privacy Rule applies to health plans, health care clearinghouses, and certain health care providers, and it also requires these covered entities to amend any business partner agreements they have in order to condition their disclosures of PHI to them.

Modern healthcare services, activities, and functions are rarely carried out in isolation. They are assisted by a variety of other businesses, alliances, joint ventures,

and contractors. A “business associate” under the HIPAA privacy rule is an individual who uses or discloses personal health information to perform a function on behalf of the covered entity. Covered entities can disclose PHI to their associates under the general consent conditions for disclosures for TPO, but only if they receive an assurance that the business associate will protect the confidentiality of the information. Disclosure is conditional on the assumption and agreement that the information will be used only for the purposes for which it was intended by the covered entity. In addition, it requires an assurance that the associate will safeguard the information from misuse and will help the facility to comply with the duties to provide access to health information and a history of disclosures to the patient as requested (Bricker & Eckler, 2001; Office For Civil Rights, 2001; Roach, 2001).

The regulations state that a business associate provides one or more of the following functions:

- Claims processing or administration
- Data analysis, processing or administration
- Utilization review
- Billing
- Quality assurance
- Benefit management
- Practice management
- Legal
- Actuarial
- Accounting
- Data aggregation
- Consulting
- Accreditation
- Financial services, or any other function or activity where the provision of the service involves the disclosure of individually identifiable health information. (HIM professionals can add functions such as transcription, coding, and release of information to the list).

A business associate is not a member of the workforce of the health care provider, health plan, or covered entity. The Secretary of HHS cautions that, “the

mere fact that two covered entities participate in an organized heath care arrangement does not make either of the covered entities a business associate of the other covered entity." For example, disclosures by a provider to another provider for consultation or referral do not need to meet the business partner requirements (AHIMA Policy and Government Relations Team, 2001a; Bricker & Eckler, 2001).

The privacy rule requires that business partners of covered entities make their internal practices, books, and records relating to the use and disclosure of PHI available to HHS for purposes of determining the covered entity's compliance. Because HHS may consider a covered entity to be in violation of the regulations if its partner is in violation, some organizations fear that the standards impose a duty on them to monitor and police their business partners. Although this is a reasonable concern, HHS has stated that there is no duty to monitor adherence or performance unless the covered entity knew or should have known of transgressions.

HHS will be modifying and adding to the HIPAA regulation. Therefore, any agreements with business partners should require the partner to negotiate amendments to the contract in good faith to accommodate any such future changes.

Assessment Plan:

- Review all current organizational relationships and functions to determine when, or if, the entities involved might become business associates.
- Review all existing entities with which NAVAHCS has vendor/business contracts to see which entities can be categorized as "business associates" for

HIPAA compliance.

- Determine which will be in effect on the relevant compliance date. NAVAHCS' contracts will need to require future business partners to make their internal practices, books, and records relating to the use and disclosure of PHI available to HHS for audit to determine compliance with the privacy regulations. NAVAHCS' future contracts will need to stipulate the right to audit and monitor business partners to confirm compliance.
- During the examination of current contracts/business agreements one must ask:
    - Is it expressly stated that the business partner may not use or disclose the PHI other than as permitted or required by the agreement?
    - Is there a specific description elsewhere in the agreement/contract of how the partner can use, and to what extent it can disclose, PHI?
    - Is there a provision in each contract that requires the business partner to use appropriate safeguards to prevent the use or disclosure of PHI, other than as provided by the agreement?
    - Is there a stipulation in the agreement requiring the business partner to report to NAVAHCS any use or disclosure of PHI in violation of the agreement?
    - Do the contracts stipulate that the business partner must ensure that any agents (subcontractors) to whom it provides PHI agree to the same restrictions and conditions that apply to the business associate?
    - Do current contracts oblige the business partner to comply with patient's right to access for inspection or copying?

- Do current contracts stipulate compliance with the right to amend or correct PHI? (The covered entity must make a reasonable effort to notify other entities of a correction. The business partner must incorporate any correction to PHI when notified by the covered entity).
- Do the contracts provide for the return or destruction of all PHI received from NAVAHCS upon termination of the business agreement? (The contractor will make no copies) (Roach, 2001; QuadraMed, 2001).

Other Requirements:

A covered entity may use the following PHI to maintain a directory of patients in its facility: the individual's name, location in the facility, religious affiliation, and condition described in general terms that do not communicate specific medial information or diagnosis.

The facility may disclose the above PHI for directory purposes to members of the clergy, or to other persons who ask for the individual by name. The facility must inform individuals of the information they may include in a directory and the persons to whom it may disclose such information. Patients must be provided with the opportunity to restrict or prohibit some or all of the disclosures. If the opportunity to object cannot be provided because of emergency treatment or incapacity, a provider may use or disclose some or all of the PHI that is permitted if the disclosure is in the individual's best interest as determined by the provider's professional judgment. As soon as the patient is capable of objecting, the covered entity must inform the individual and provide an opportunity to object (AHIMA Policy and Government Relations Team, 2001a).

Assessment Plan:

- Does NAVAHCS maintain a facility or patient directory? (Is this more than the daily gains and losses statement?) If so:
    - How is it compiled?
    - What information is included?
    - How is it updated?
    - Who has access to the directory to release information?
    - Are there current polices or procedures in place regarding a facility directory?
- Does NAVAHCS have a regulation that allows patients to be excluded from the directory or to place restrictions on the information released?
- Is the "opt-out" restriction/opportunity a part of the registration process?
- Is the right of the patient to opt-out of a facility directory integrated into the *Notice of Privacy Practices* that describes the uses and disclosures of PHI that it is permitted to make?
- Does NAVAHCS have a designated person who is to be contacted in the event a patient is unable to opt-out of the facility directory? (Bricker & Eckler, 2001).

<u>Use and disclosure for involvement in the individual's care and notification purposes:</u>

A covered entity may disclose to a family member, close personal friend, or any other person designated by the patient, the PHI that is directly relevant to its involvement with the patient's care or payment. If the patient is present and has the capacity to make health care decisions, the hospital may use or disclose PHI if it obtains the patient's consent or provides the patient with the opportunity to object to the disclosure.

If the patient is not present or does not have the opportunity to agree or object to the use or disclosure because of emergency or incapacity, the covered entity may determine whether the disclosure is in the best interest of the individual. If in the exercise of professional judgement, an agent of the covered entity chooses to disclose,

he must disclose only the PHI that is directly relevant to the person's involvement with the patient's healthcare. This enables the facility to make a reasonable inference concerning the patient's best interest in allowing a family member or other person identified by the patient, to pick up medications, x-rays, or medical supplies (AHIMA Policy and Government Relations Team, 2001a).

Assessment Plan:

- Is there a protocol to inform patients on admission regarding disclosure of PHI to family members or significant others?
- Is there a process for patients to request that NAVAHCS restrict disclosures to family and friends involved in their care?
- Does NAVAHCS have documentation policies that require the facility to document all restrictions and termination of restrictions?

Marketing (§164.514): Marketing has a special definition in healthcare, when the privacy rule is applied to it. Marketing is defined as making a communication about a product or a service, in order to encourage those who receive the communication to use or purchase the service or product. In the HIPAA standards, certain activities that would generally be defined as marketing are not considered to be marketing in order to "prevent interference with essential treatment or health-related communications with a patient". Although the regulations do require that a covered entity may not use or disclose PHI for marketing without authorization from the patient, there are notable exceptions. If the covered entity communicates in order to provide or manage further treatment, such as sending reminder notices for appointments or mailing prescription refills, it is not considered marketing. Describing participating providers or plans in a network, or describing the services and benefits they provide, is not considered

marketing under the privacy rule. Another significant exception applies to communications that are specifically tailored to the circumstances of a particular patient, and are made by a health care provider to that patient as part of his treatment. This would include disease-specific mailings or other communications for the purpose of directing or recommending alternative treatments or therapies (Bricker & Eckler, 2001; Gue, 2001)

Marketing as defined above does not apply to VHA, and, therefore, does not apply to NAVAHCS. Because the VHA does not receive direct or indirect remuneration from a third party to encourage the use of a service or product, it does not conduct marketing (VHA Office of Information, 2001).

(State Law Preemption: §160.203

State preemption is addressed in the final rule. Any "standard, requirement, or implementation specification adopted under the [Rule] that is contrary to a provision of State law preempts the provision of State law" (AHIMA Policy and Government Relations Team, 2001b, p.1).

Compliance regulations require that healthcare providers themselves determine whether the federal requirements preempt existing state privacy laws. Under HIPAA, state laws prevail if they are "more stringent" than the federal law. Providers that are located or work in more than one state may encounter significant challenges when defining and determining the rules concerning situations that are unclear or are multi-jurisdictional. Compliance will require complex evaluation to determine which law applies (American Hospital Association, 2001a).

The preemption of state law remains one of the more controversial issues surrounding HIPAA. There are those groups that support complete preemption,

creating a federal “ceiling” to establish a uniform national standard for the release and disclosure of PHI. States then could not enact more stringent laws. Other groups support the creation of a federal “floor” of protections where states would have the ability to pass strong laws that would supersede federal law (AHIMA Policy and Government Relations Team, 2001b).

Analysis of the preemptive effect will be a complicated and difficult task for non-federal facilities and will require discrimination to determine whether a state law is subject to preemption.

VHA as a federal agency is not subject to state law. The state preemption therefore does not apply to NAVAHCS (S. Putt, personal communication, October 22, 2001).

The Security Standards

Security establishes the methods by which an organization protects, restricts, and limits access to confidential patient information. The proposed HIPAA standard for the security of health information was first published in 1998 and requires healthcare entities to assess their own security needs and risks and devise, implement, and maintain appropriate security (Cassidy, 2000a).

The original HHS security rule covered only electronic patient-identifiable health data. This has since been expanded to cover paper and oral records that are either the source or the progeny of an electronic record. The rules require a covered entity to have in place appropriate administrative, technical, and physical safeguards that protect against unauthorized access and misuse of electronic information.

The rules are flexible and do not specifically prescribe the measures that a facility must take to meet the standard. They are designed to be “scaleable” but require that

information security must also be comprehensive. HIPAA expects each facility to address cultural and organizational issues, as well as the technological and physical concerns. The rule, (45 CFR Section 164.530(c) Safeguarding Protected Health Information), states that each entity must reasonably protect patient information from any intentional or unintentional use or disclosure that is in violation of the standards or other requirements of the regulation (Bricker & Eckler, 2001). The Security Rule emphasizes both external and internal security threats.

HIPAA required the Secretary of HHS to create standards for administrative and financial healthcare transactions related to healthcare. In order to be in compliance, the standards must be met in all areas (Cassidy, 2000b). Health claims or equivalent encounter information include the following types of transmissions:

- Health claims attachments
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Healthcare payment and remittance advice
- Health plan premium payments
- First report of injury
- Health claim status
- Referral certification and authorization

HIPAA Security Standards Categories:

The safeguards that constitute HIPAA mandated security focus on the protection of individually identifiable health information through the following four ways:

1. Administrative Procedures §142.308(a): These are defined as formal, documented practices to manage the selection and execution of security measures to protect data as well as direct the conduct of personnel in relation to the protection of data. The administrative procedures are intended to limit information access to appropriate parties and guard information from all others. There are twelve areas in which policies and

procedures must be implemented and maintained:

1. Certification – the technical evaluation of the compliance of data systems.
2. Chain of Trust Partner Agreements – an agreement between a covered entity and all other organizations with whom they share health information to “protect the integrity and confidentiality” of all identifiable health information.
3. Contingency Plan – a documented plan to maintain the continuity of operations in case of a disaster or emergency.
4. Formal Mechanism for Processing Records – policies and procedures for the receipt, handling and disposal of health information.
5. Information access control – policies and procedures for allowing different levels of access to health information.
6. Internal Audit – regular review of systems access patterns.
7. Personnel Security – policies and procedures such as security clearances, access record maintenance, and staff training.
8. Security configuration Management – procedures that coordinate the overall operation of security.
9. Security Incident Procedures – measures for reporting and responding to security incidents.
10. Security Management Process – a process to “ensure the prevention, detection, containment and correction” of security breaches.
11. Termination Procedures – procedures used when terminating employees or users to prevent continue access to health information.
12. Training – security awareness training for all personnel, and specific training of users on system security protocols.

(Gue, 2001).

Assessment Plan:

- Are contingency policies in place that address and identify the data and applications most critical to NAVAHCS (direct delivery of care, life support, vital environmental systems)?
- Does NAVAHCS have a data backup plan? Has documentation been developed detailing frequency, extent, storage, and the responsible parties?
- Does NAVAHCS have an emergency mode, operation plan that addresses the information infrastructure?
- What systems are supported by emergency power and how long does the power last?

- Is there a replication of the critical systems in a remote location and how long does it take to bring it online?
- Is replication built into the network?
- Are vendors able to supply new hardware in a timely manner?
- What processes are in place for switching back to manual procedures? Are staff aware of and trained in manual backup procedures?
- Is there a risk analysis policy, a risk management policy, a sanctions policy, and a general security policy in place?
- Is there a policy/process in place to report breaches of security? If so, does this policy define what events are reportable as an incident; who must report an incident; how it should be reported, and to whom?
- Is there a process in place that describes the appropriate response to an incident and how security incident reports are used to improve the overall security of the system?
- Are employees instructed in how to report breaches?
- Do employees, students, and volunteers receive specific training about the confidentiality of health information and sign a confidentially agreement at the time of employment?
- Does NAVAHCS have a policy prohibiting the disclosure or sharing of passwords, access codes, or other user identifiers?
- Does the information system limit mass copying, printing, or downloading of patient records?
- Does NAVAHCS have a policy that prohibits employees from loading unauthorized software into the organization’s computers?

- Does NAVAHCS require contractors or vendors who provide services that involve health information to sign confidentiality agreements and have confidentiality statements on file for their employees or agents?
- Does NAVAHCS have chain of trust agreements (a contract entered into by two business partners in which the partners agree to electronically exchange data and protect the confidentiality of the data exchanged) with all third parties that have access to patient health information? If so, do the agreements state that the third parties will:
    - Keep the information in strict confidence?
    - Use the information only for the purpose of providing services under the contract?
    - Disclose the information only to those employees who need access to the information in order to provide services under the work contract?

(Brandt & Carpenter, 2000; Fuller, 1999; QuadraMed, 2001).

2. Physical Safeguards §142.308(b): This section refers to the physical computer systems and related buildings and equipment that must be protected from natural and environmental hazards, as well as from sabotage or intrusive acts. It addresses facility and workstation security, physical control of media storage and disposal, and visitor/maintenance authorization and escort (Office of Information HIPAA Coordinator, 2000). There are five areas of physical safeguards:

1. Assigned Security Responsibility – officially assigning accountability for physical safeguards.
2. Media Controls – setting up formal procedures for controlling and tracking the handling of hardware and software, data backup, storage, and disposal.
3. Physical Access Controls – developing a facility wide security plan and setting up emergency and disaster plans.
4. Workstation Use – developing policies and procedures to prevent unauthorized

access to protected information on terminals.

5. Security Awareness Training – educating all employees and others who have access to protected health information.

(Gue, 2001)

Assessment Plan:

1. Evaluate the physical operations and assess vulnerabilities.

    - Are rounds routinely conducted to assess physical access controls?
    - What safeguards are in place to protect equipment from vandalism or theft?
    - What precautions are taken for a physical disaster, such as flood, fire, bomb threats, power outages, earthquake, etc?
    - Does NAVAHCS have any special physical security procedures in place for computer rooms or network closets? Are they locked? Are only a limited number of people given access to these areas?
    - How are system back-up tapes prepared and delivered?
    - How is personally identifiable health information disposed of?
    - If inactive paper-based or computer-based records are archived, are they protected from loss, damage, or unauthorized disclosure?
    - Is there a documented process of periodic testing to identify areas of weakness?
    - Are paper records stored under lock and key and returned to a secure place after hours?
    - Are charts left in exam rooms or any other place where other patients are waiting for their appointments?
    - Are paper records disposed of in-house with a shredder?
    - Does staff receive training/education about the elements of physical security,

including the importance of confidentiality and information security?

- Does staff receive job-specific training in information handling?
- Is there a policy in place that addresses the faxing of health information? (Use of a cover sheet, patient authorization when necessary, steps to follow if a fax is sent to the wrong destination)
- Are all fax machines located in secure areas where access is limited to appropriate staff?
- Are all incoming documents monitored so they can be routed immediately in a secure fashion?
- Does staff receive training in how to report a breach?
- Is there a personnel security policy in place that includes pre-employment clearance checks? Does there need to be in a VHA facility?
- Is there a policy in place that describes processes related to the termination of an employee? (i.e. denying physical access, removal from active user accounts on all systems, return of keys for computer rooms)
- Is there a designated person responsible for an information security program?

(Dennis, 2000; Fuller, 1999; QuadraMed, 2001).

3. Technical Security Services §142.308(c): These are processes that must be implemented to protect and control information and monitor individual access to information. This component is designed to enforce administrative policies. Services to monitor will include access, audit trails, authorization control, data authentication, and entity authentication. These methods should authenticate the user and also restrict the user to those systems and data for which he is authorized. Included in technical security services are:

- Access Control – limiting access to those with valid needs and authorization.
- Audit Controls – setting up system mechanisms that record and monitor activity.
- Authorization Control – obtaining and tracking the consents of patients for the use and disclosure of health data.
- Data Authentication – ensures that data are not inappropriately processed, altered, or destroyed.
- Entity Authentication – employs mechanisms such as passwords, automatic logoff, or PINS, which identify authorized users (Gue, 2001).

Assessment Plan:

Are policies in place that address and describe record processing and electronic healthcare transactions?

- Do the policies address the receipt of data, manipulation, storage, dissemination, transmission, and disposal of data?
- Is anti-virus software used to help detect and block computer viruses and other forms of sabotage?
- Who is responsible for the maintenance of electronic record systems? Does NAVAHCS have a designated individual?
- Does NAVAHCS utilize an access matrix that determines, by staff role, what desired access levels should be?
- Do terminals that are routinely used to access health information have “timeouts”? (i.e. an interval defined in seconds to control the length of time a computer will wait for a user to respond to a “read”, or the maximum time allowed after no keyboard activity to prevent unauthorized access to unattended terminals.
- Does the access control system assign protection levels to individual data elements within each directory or file?
- Does NAVAHCS have technology that ensures that only authorized entities gain access to network resources?

- Does the Information Systems Service Line (ISSL) have a process to protect E-mail that contains sensitive or confidential information from unauthorized access, alteration, or disclosure?
- Does the Information Security Service Line (ISSL) have an audit mechanism in place (and a policy) that records and examines system activity?
- Are logins, file accesses, and security incidents monitored?
- Does ISSL keep records of security transactions that could verify granting, modifying, or terminating privileges?
- Are procedures in place to document receipt and transmission of electronic records?
- What process does NAVAHCS have for adopting new technology?
- Who makes purchase decisions and assesses the potential risks?
- Are policies updated when new technology is adopted?
- Are employees notified of policy changes?

(Computer Based Patient Record Initiative (CPRI), 2001; Dennis, 2000; Fuller, 1999; Zender, 2000).

4. Technical Security Mechanisms §142.308(d): This provision addresses the protection of patient data from access by public networks. This includes wide area networks, remote access (dial-up), Intranet, and Internet approaches. Appropriate security requires communications/network controls, including monitoring the use of the Internet, encryption, firewalls, and virus protection. This section also mandates on-going threat, penetration, and vulnerability audits (Beacon Partners, 2001). Controls to prevent transmitted health information from being intercepted via external entry points are:

- Integrity Controls – internal verification that stored and transmitted data are valid.

- Message Authentication – assurance that the messages sent and received are the same.
- Either Access Controls – dedicated secure communication lines; or Encryption, which transforms text into ciphers through the use of a special algorithm process.
- If using a network, protections must also include alarms, audit trails, entity authentication and event reporting (Gue, 2001).

Assessment Plan:

- Has NAVAHCS created a network diagram including the location of remote access points (Internet gateways), the number of remote users, and remote locations?
- Are Internet gateways protected with authentication and by firewalls?
- Are all dial-up points beyond the firewalls protected with strong authentication?
- Are non-essential services on servers disengaged?
- Are security devices at NAVAHCS routinely patched?
- Are there intrusion detection systems to monitor traffic through access points?
- Does NAVAHCS have technology or some other process to create alarms in the event of suspicious network activity?
- Does ISSL identify new vulnerabilities and install patches to security devices immediately upon release to staff?
- Does ISSL frequently review firewall logs, intrusion detection alerts, and other data sources to identify potential security breaches?
- Does ISSL routinely report and document any instances of suspicious activity and security device malfunctions?
- Is there a policy in place that defines which events are reportable, who must report a security incident, how it should be reported, and to whom?
- Does NAVAHCS ensure that all security devices are upgraded promptly and configured optimally? (Security Configuration Management is listed under the

Administrative Procedures section in the HIPAA Security and Electronic Signature Standard.)

- Does NAVAHCS have a policy covering the receipt, and removal of hardware and software?
- What files and processes need encryption? Should all patient-related transmissions to remote locations be encrypted?
- Is personal software permitted at NAVAHCS? How does ISSL review the software license before loading to make sure the additional copy doesn't place the hospital at risk of a licensing violation? How have employees been notified of the need to check with ISSL first?

(Dennis, 2000; Fuller, 1999; Higgins, 2000)

Expected Findings and Utility of Results

Compliance with HIPAA mandates will compel health care providers to profoundly change the way they do business. New administrative burdens and expenses will be an initial encumbrance, but engaging proactively in compliance efforts will lessen the burden.

This project will evaluate NAVAHCS' current compliance status with HIPAA requirements as it relates to the privacy and security standards in the final rule. An understanding of current policy and practices provides a prediction of the expected results of the study.

The legal right to access, copy, and amend patient health records has been present in the VHA and other federal healthcare organizations for decades. The Privacy Act of 1974 granted patients a measure of control over personal health information collected and maintained by the government. The Act affords patients the

right to discover what information has been collected about them and to correct or amend it if it is demonstrated to be factually inaccurate (Hughes, 2001). The VHA is bound by the Act's provisions, which in some areas are more stringent than those required by HIPAA (Stewart, 2001). There are instances however, where the Privacy Act is less open as it relates to individual rights. In these situations, the legal authority that affords the patient with more rights or more access will be the deciding authority. For all administrative requirements, VHA will comply with both the HIPAA Final Privacy Rule and with the Privacy Act (U.S. Department of Veterans Affairs, 2001). In those areas directly associated with and applicable to the Privacy Standards, it is expected that NAVAHCS will be in good standing.

Evaluating security methods and risk assessment protocol will be pertinent and timely in light of the proposed HIPAA security mandates. The VHA has made a good beginning at replacing its mountains of paper records with electronic data and digitized material. When there are inconsistent security measures protecting them, these multimedia records can lead to breaches of confidentiality. Interpreting and complying with the Proposed Security Rule may be less difficult for NAVAHCS than for many private sector facilities because it currently operates under the Computer Security Enhancement Act of 1997. VHA also has a Medical Information Security Service (MISS) and an established information security program in place, as well as a security training awareness curriculum (Burks & Collins, 2001).

Recently, the VA received disturbing news from the Government Accounting Office (GAO). Auditors disclosed that there were problems in the IT security "architecture." The House Committee on Veterans Affairs, Subcommittee on Oversight and Investigation also concluded that the VA suffered from "deficiencies" in several

major areas, including inadequate security controls, inadequate controls over access, software applications, system software, segregation of duties, and others (Walsh, 2001). The implications for information security management to effectively coordinate cyber security standards are imposing (GAO Testimony, 2000).

NAVAHCS successfully identified and addressed all Y2K associated issues related to clinical and administrative processes. This provides a basis for predicting the current security status of the facility's information systems. It is expected that after a thorough review of the regulations with appropriate IT personnel, NAVAHCS will be in an excellent position to identify and prioritize the necessary changes to policies and procedures for effective HIPAA compliance.

Bruce Brody, Associate Deputy Assistant Secretary for Cyber Security, Department of Veterans Affairs, when discussing the implementation of HIPPA standards in light of a restricted budget and capital investing process, stated that some compliance trouble areas were "money neutral." He stated that, "technology isn't necessarily the first answer, sometimes it is a ***process*** (emphasis added) itself that needs to be followed more carefully" (Walsh, 2001, p. 10).

For this reason, the assessment plan outlined in this proposal has extensive utility. Examining each department through the lens of HIPAA will provide participating service lines with a better understanding of what constitutes a questionable process or a suspected or potential breach. Sharing the results of investigation and analysis with service line managers will present new challenges and many opportunities to identify security and privacy rifts.

It is expected that a clearer perception of administrative, clinical, and technical risks throughout the facility will result from this research. In this way a useful and

practical gap analysis can be conducted.

This project has been conceived and devised to provide a necessary and applicable instrument for NAVAHCS to use in addressing HIPAA compliance. This is the initial phase in standardizing the management of individually identifiable health information. As the assessment methods are refined it may potentially develop into a serviceable tool to create a compliance assessment framework that can be shared with other facilities within the VISN.

Gap Analysis

Complying with HIPAA is one of the most challenging issues facing the health care industry today. In the private sector, it represents the first major intrusion of the federal government into what has been a traditionally state regulated domain. In the race to prepare for HIPAA, strategic financial planners are concerned about the significant funds they will need to commit to the renovation of computer systems and the hiring of consulting firms. There is a deluge of vendor proposals from consulting firms offering to help with compliance, but HIPAA cannot be implemented in isolation solely by upgrading computer systems. It will require a change in corporate culture and staff behavior as well as a thorough examination of each facility's security and confidentiality policies (Weber, 2001).

The following analysis will address the questions asked in the assessment plan under each section in Methods and Procedures. Answers to the assessment questions will provide a comparison of current procedures and policies for the use and disclosure of health information with the proposed privacy and security standards.

This project will examine the following areas; consent, authorization, right of access and amendment, uses and disclosures for public health activities, business associate agreements, use and disclosure for involvement in patient care, and other requirements under the Privacy Standards. It will examine administrative procedures, physical safeguards, technical security services, and technical security mechanisms under the Security Standards. NAVAHCS must determine which areas need attention in order to achieve HIPAA privacy compliance.

Standards for Privacy of Individually Identifiable Health Information:

(45 CFR Parts 160 and 164)

Assessment Points:

NAVAHCS has already designated both a Privacy Officer and a Security Officer. Ms. Sharon Chapman, Health Information Management (HIM) Service Chief is the appointed Privacy Officer, and Mr. Jim Orey in the Information Systems Service Line (ISSL) is the appointed Information Security Officer.

Currently, the Privacy Officer and the Information Security Officer, working closely with the Staff Development Department and Human Resources, are jointly providing training related to confidentiality of protected health information and computer security during each month's orientation for new employees. This format can easily be expanded at the beginning of the next fiscal year to include HIPPA-specific elements and facility-wide education to be in compliance with the employee-training requirement. It might then be included in the mandatory educational modules available on the Intranet for annual training.

The Computer Security Act of 1987 requires mandatory, periodic training in computer security awareness. NAVAHCS employees attend an automated information system (AIS) security awareness class during orientation for new employees, and they receive other security training annually in accordance with Office of Personnel Management (OPM) Regulation 5 CFR Part 930. During the training, it is emphasized that all employees who handle sensitive information have a legal and moral responsibility to prevent unauthorized disclosure. Each employee signs a statement of understanding that defines access privileges and acknowledges responsibility. This

mandatory instruction is also required according to the VA Directive 6210 (Automated Information Systems Security).

The Medical Center Memorandum, MCM NO 00-16, “Statement of Organizational Ethics” was established in recognition of the ethical responsibility a health care organization has to the patients and community it serves. This policy describes a code of behavior for employees and provides an ethical framework for patient care and business operations. It emphasizes that it is the responsibility of every employee and volunteer to act in a manner consistent with the intent of this organizational statement and its supporting policies. NAVAHCS clearly defines its responsibility to respect patient privacy and maintain PHI in a confidential manner to be used only by those individuals authorized to review and act upon this information.

Procedures for determining position sensitivity levels and setting limitations on access to and use of PHI are activated when staff are hired and are outlined in MCM NO. 15-26, “Automated Information Systems (AIS) Security Policy”. The provisions in this memorandum comply with Federal AIS security laws and regulations, including the Computer Security Act of 1987.

The Privacy Act of 1974 delineates legislative prohibitions against unauthorized disclosure of protected information. An employee or volunteer who unlawfully gains access to a record, when there is not a need to know, or who willfully discloses information to any person or agency not entitled to receive it, is subject to civil action and criminal penalties and can be fined up to $5000 (MCM NO. 15-20, 2002). All NAVAHCS employees are asked to sign an Information Security Notification which states that violations or major or repeated transgressions will result in appropriate disciplinary action as defined in VA employee conduct regulations (VAR 820(b)).

During orientation and the annual mandatory security and confidentiality training, employees are instructed to inform the Privacy Officer or the Information Security Officer about perceived violations of privacy or security. Reminders are provided in Microsoft Outlook and the Veterans Health Information Software and Technology Architecture (VistA computer system) e-mail and are sent to all employees on a regularly scheduled basis. The Inspector General conducts or provides oversight for criminal investigations, as appropriate (VA Directive 6210, 1997).

The Freedom of Information Act also directly addresses privacy issues. There are policies in place that set limitations on access to and use of protected health information according to what an individual needs to know. An employee or volunteer who unlawfully gains access to a record in performance of his duties, when there is not a need to know, or who willfully discloses information of a personal nature to any person or agency not entitled to receive it, can be fined (Medical Center Memorandum N0. 15-20, The Privacy Act of 1974). NAVAHCS submits an annual Freedom of Information Act report concerning disclosures of protected health information for purposes other than treatment, payment and healthcare operations.

Consent: 45 CFR § 164.506

The consent requirements are to some extent defined by the definition of the covered entity. According to HIPAA, the VHA is both a health plan and a health care provider under the provisions of Title 38, United States Code. The discussion here is limited to consent related to NAVAHCS as a health care provider. In its role as a health care provider, NAVAHCS is required to obtain an individual's consent to use or disclose protected health information. The Office of Information Workgroup states that as a health care provider, obtaining one consent to cover all VA Medical centers, Outpatient

Clinics, Nursing Homes, CBOC's, and other facilities that support the delivery of health care is administratively preferable and recommended (Office of Information, 2001).

At this time NAVAHCS does not have a separate *Notice of Privacy Practices.* The explicit information HIPAA requires in such a document is not included in any other document. There is a *Consent to Release Information* section on the Instructions for Completing Applications for Health Benefits (VA Form 10-10EZ), as well as a *Request for and Consent to Release of Medical Records Protected by 38 U.S.C. 7332* (VA Form 10-5345(R). These *Consents* do not state that the patient has a right to restrict how his PHI is used or disclosed to carry out treatment, payment or health care operations. They do state that the patient has the right to revoke *authorization* at any time, except to the extent that action has already been taken to comply with it. They also state that without an express revocation by the patient, the consent will automatically expire when all action arising from the VA's claim for reimbursement for care has been completed. It is expected that the VHA Project Management Office will coordinate the drafting of a standardized *Notice* for dissemination to all VA Medical Centers sometime this year. A decision and policy on how the *Notice* will be disseminated to veterans is also forthcoming and, depending on the method of distribution, the cost may be high (Department of Veterans Affairs, 2001, September). The responsibilities and procedures for obtaining and documenting informed consent are explained in MCM NO. OQ-12, "Informed Consent". This includes a discussion of surrogate decision-makers, substituted judgment, health care agents, legal or special guardians, and next-of-kin. In medical emergencies, the patient's consent is not required, but the signature must still be obtained after the clinical intervention when necessary.

HIPAA requires retention of signed consent copies for six years from the date of creation or when it was last in effect, but NAVAHCS retains records for three years in our own facility before they are transferred to the Federal Record Center for 72 years.

Authorization: §164.508

This section of the final privacy rule states that covered entities may not use or disclose protected health information without a valid authorization, except as otherwise permitted or required in the rule.

NAVAHCS does not have a specific *authorization* form that contains the required core elements for compliance. Because VHA is an entitlement program, it is precluded from refusing care to eligible patients regardless of their willingness to provide an authorization form. However, in order to determine eligibility, it is necessary to provide information to the VA in order to process the request and so serve the individual's medical needs. This is detailed in the *Privacy Act Information* section on the eligibility application.

When NAVAHCS requests information and authorization from another covered entity to disclose PHI to this facility in order to perform TPO, a cover sheet and signed patient consent for release of information accompanies the request.

VHA is compliant with HIPAA authorization standards in that it addresses expiration and revocation of authorization and does not combine authorizations for multiple uses.

Right of Access and Amendment: (§164.524 and §164.526)

Any individual may request amendment of any DVA record pertaining to him, and this request must be acknowledged in writing within 10 working days after receiving the request. The necessary review of the record will be completed as soon as reasonably

possible, (normally within 30 days) unless unusual circumstances preclude completing the request within that time. The record will then be corrected, either in whole or in part if the patient demonstrates that it is not accurate, relevant, timely, or complete. If the request is denied, the individual will be informed of the refusal to amend the record, the reason for the refusal, and the procedures to request a review of that refusal (VA FOIA Regulations 40 FR 33944 §1.579).

By following current policies and procedures covered under the Privacy Act and FOIA, NAVAHCS is overall partially compliant with this section. MCM NO.15-20, "The Privacy Act of 1974 – Release of Information", permits individuals to request access to inspect or obtain a copy of their PHI, and it designates which record sets are subject to access and amendment by which individuals. The policy documents the titles of persons and offices responsible for receiving and processing requests and processing responses to a review of denial. All individuals or third parties requesting access (in writing) to individual records maintained at this facility are required to provide the requisite information and verification of identity. The health administrative specialist or his designee will indicate at that time if access will be granted. If not, the reason will be given and a date and time established when the review could be made. The medical center director is the reviewing official for all denial to access, review, correction, or amendment of records (MCM NO.15-20, 2002).

This Memorandum also discusses the appropriate response to requests for PHI that do not require consent, such as the release of information to federal, state, county or local government agencies. NAVAHCS staff is informed as to when it is appropriate to deny a request for access, and this process is directed and managed by the Privacy

Officer. Staff is never permitted to release information without direction from the Chief of HIMS (the Privacy Officer).

NAVAHCS has a process to create and provide an audit trail for patients when PHI has been disclosed for purposes other than TPO. There is a monthly *Release of Information* report that has requests by type and includes how many are open and how many requests have been closed.

VHA already requires a faster response than does HIPAA, but it does not have a policy in place for showing requests and denials for releases of PHI. According to the VHA Privacy Subgroup, the VHA will probably choose not to provide written rebuttals, nor does VHA uniformly send amended PHI to other covered entities (VAMC Executive Summary, 2001).

Uses and Disclosures for Public Health Activities and Disclosures About Victims of Abuse, Neglect, or Domestic Violence: §164.5129c

Under the provisions of 38 U.S.C. 3301(e) and (f) 2, and consistent with the Privacy Act, information may be released from patient medical records to officials of any governmental agency charged under applicable law with the protection of public health or safety (MCM NO. 15-20, 2002).

Standing requests rely on state's reporting statutes and regulations and are designed to protect the public health or safety. Notifications to appropriate authorities may be made of treatment for gunshot wounds, diagnosis of communicable diseases, and incidents of suspected abuse and neglect. Agencies must update their requests in writing every four years (MCM NO. 15-20, 2002). The NAVAHCS Police and Security Manager have established current Memorandums of Understanding with the local law enforcement agencies authorizing the release of personal information to them when

they are conducting an official police investigation. However, any past or present information relating to a patient in a drug dependence or alcohol treatment program will not be released without a court order or a “special consent” obtained from the person whose record is involved. All requests for release of medical information containing drug abuse, alcoholism or alcohol abuse, infection with HIV or sickle cell anemia are forwarded to Release of Information (ROI). Disclosures may be made only when the individual has provided specific written consent for disclosure; e.g., VA Form 10-5345 (R) (MCM No. 15-20).

NAVAHCS does not account for all these disclosures at this time. Records are not kept documenting transactions with local law enforcement agencies.

Business Associate Agreements: [45CFR §§ 160.103, 164.502(e), 164.514(e)]

The final rule imposes substantial requirements on covered entities with respect to their business associates. There is still significant confusion regarding many of these requirements. HIPAA is concerned with establishing standards that will ensure that the use and disclosure of PHI by a covered entity’s business associate is appropriately protected. HHS contended that the privacy standards would be meaningless if a covered entity could circumvent the requirements by contracting out the performance of operations covered by the standards (Gradle, 2002). Contracting policies will be addressed at the national level and guidance to the individual facilities will be disseminated by VHA.

Some VA divisions such as the Veterans Benefits Administration that provide support or services to VHA meet the definition of a business associate, and, as such, they must comply with the requirements of the Final Privacy Rule. VHA also shares information in accordance with the Privacy Act with other federal agencies, such as the

Department of Defense. In some circumstances the federal agency would not be a business associate. However, the information sharing practices allowed under the final Privacy Rule, especially with the DOD will need to be evaluated further by the OI HIPAA Workgroup or by an established VHA HIPAA Project Management Office (VHA OI HIPAA Workgroup, 2000).

Current contractual language does not require compliance from business associates. However, under the Privacy Act a clause is to be inserted in a contract when the design, development, or operation of a system of records for individuals is required to accomplish an agency function. In operating any system of records, the contractor then must agree to comply with the Privacy Act and the agency rules and regulations issued under it. The contractor also agrees to include the Privacy Act notification in every solicitation and resulting subcontract when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records subject to the *A*ct.

Operation of a system of records means the performance of any of the activities associated with maintaining the system of records, including the collection, use and dissemination of records. *Record*, is defined as any item, collection, or grouping of information about an individual that is maintained by an agency, including financial transactions and medical history. *System of records on individuals*, means any group of any records under the control of any agency from which information is retrieved by the name of the individual, or other identification assigned to the individual (Privacy Act § 52.224-1.52.224-2*).*

A civil action may be brought against the agency involved when a violation concerns the operation of a system of records of an individual. Criminal penalties may

be imposed upon the officers or employees of the violating agency. The Department of Health and Human Services, Office for Civil Rights has been delegated the authority to enforce the privacy rule (Office for Civil Rights, 2001).

In at least some of the current contracts written by the NAVAHCS Contracting Officer, security is addressed in detail. NAVAHCS provides designated contract employees with the same access to the Veterans Health Information Systems and Technology Architecture (VistA) computer system as the professional staff of all VA operated facilities. All employees accessing the system are required to sign and abide by all VA security polices and applicable confidentiality statutes such as 38 U.S.C. 5701, 38 U.S.C. 7332, and the Privacy Act. All contractor employees who require access to DVA computer systems are subject to a background investigation and must receive a favorable adjudication from the VA Office of Security and Law Enforcement. This requirement is applicable to all subcontractors who access PHI as well.

VA facilities must ensure that appropriate security requirements are included in statements of work and are implemented properly before the system goes into operation. Approving officials ensure that all information resource sharing agreements pertaining to computer hardware and software are reviewed for security implications. They are also responsible for including the requirements in the agreement dealing with information security issues. (MCM NO.15-26, 2002). The Contracting Officer inserts the pertinent clauses in contracts for information technology, i.e., contracts which require security of information technology or are for the design, development, or operation of a system of records using commercial information technology services or support.

To ensure compliance with HIPAA legislation, business processes will need to be adapted to track and maintain business associate contracts. Contracts with NAVAHCS

will need to obligate future business partners to make their internal practices, books, and records relating to the use and disclosure of PHI available to NAVAHCS and HHS (when necessary) for audits to determine compliance with the privacy regulations.

Use and disclosure for involvement in the individual's care and notification purposes:

The NAVAHCS does not have a written protocol to inform patients on admission of disclosure of health information to family members or to care givers involved in the individual's care. According to the Privacy Act, as interpreted in MCM NO.15-20, this would be a "routine use" disclosure that does not require prior written consent. Communication with the next-of-kin or a significant other regarding the patient's condition to the extent necessary in keeping with good medical/ethical practices is allowed. Providers, however, are more cautious now and often request a power-of-attorney or an oral consent from the patient before sharing information about treatment with significant others. Oral consents are then documented in the Progress Notes. A formal policy will need to be established that allows patients to request that disclosure of their health information be restricted (G. Melvin, MD, personal communication, January 8, 2002).

Other Requirements:

The NAVAHCS does not maintain a facility directory or patient directory. It does have a daily gains and losses statement and a description of every patient seen in urgent care or admitted to the hospital. The station telephone operators direct inquiries about patients to the hospital unit where they are admitted, the release of information/medical records department, the primary care team, or the administrative officer of the day, unless instructed otherwise. If instructed that the patient requests all

personal health information be restricted, the station operators will not release any information about the patient's admission status.

Currently, NAVAHCS does not require prior written consent for reports requested by the public concerning a patient's general condition (improved, unchanged, etc.) (MCM N0.15-20, 2002). This area is not in compliance with HIPAA standards.

Answers to the assessment questions regarding privacy revealed a mixed result. This is not unexpected because NAVAHCS currently complies with some standards that have greater stringency than those required by HIPAA. The gaps in compliance provide areas to be addressed.

The second area of examination for this project is compliance with the HIPAA security standards. As with privacy, the answers to the assessment questions in the Methodology and Procedures Section provide the basis for this analysis. This will be divided into the areas of administrative procedures, physical safeguards, and technical security services and mechanisms.

The Security Standards

The HIPAA security standards are still not finalized. They are included in this project because the regulations reflect best practices in security and because the privacy requirements mandate that technical and physical controls be in place to safeguard health information. Because of this imperative, many organizations are addressing the security requirements with the privacy requirements (Wilson & McPherson, 2002).

An effective system for securing the integrity of protected health information while still maintaining an appropriate level of availability of information must allow access to information by authorized personnel. It must have policies that determine who is

authorized and must employ a strong user authentication system (Katz, 2000).

Documentation of protected health information at the NAVAHCS may be on paper or in a computer based patient record, including the Veterans Health Information Systems and Technology Architecture (VistA). NAVAHCS is in the process of transitioning from paper to a fully electronic patient record. Consolidated health records are the property of the DVA, and NAVAHCS is responsible for safeguarding the record and its contents. The administrative management of patient records is the responsibility of the Information Systems Service Line (ISSL), but each clinical and support service line that contributes to the content of the patient record has responsibility for the clinical management of the record. In accordance with the Privacy Act, medical records are confidential and will not be accessible to or discussed with unauthorized persons (MCM NO.15-17).

Administrative Procedures § 142.308(a):

OMB Circular A-130, "Management of Federal Information Resources" and VA Manual MP-6, "Automatic Data Processing" require that appropriate contingency plans are developed and maintained. Service line managers are required to conduct tests on the components of the plan for which they are responsible and to update the components as required.

There are contingency policies in place that address and identify the data and applications most critical to NAVAHCS. MCM NO. 15-26, "The Automated Information Systems (AIS) Security Policy", describes a contingency plan that covers emergency response plans, backup plans, and recovery plans and identifies the roles and responsibilities of all involved staff. The information systems service line manager is responsible for addressing adverse events that impact all critical applications and for

creating and storing copies of systems, utilities/support, applications software, data files, and associated documentation for use in backup and recovery operations (MCM NO. 15-24, 2002). Critical systems are backed up daily and the backup removed from the computer room. They can be reloaded within 30 minutes, however, replication is not built into the network. The system provides a backup process that can be performed in a dynamic mode so that it can be operational 24 hours a day and a recovery feature to assure no data loss after system failure. The VISTA server system is supported by emergency power for approximately 15 hours (VHA OI Technical Services, 2001).

The NAVAHCS has a process in place to report security incidents that define what events are reportable as an incident, who must report the incident, how it should be reported, and to whom (MCM NO. 15-26, 2002). All employees are instructed in their orientation of the appropriate response to an incident and how security incident reports are used to improve the overall security of the system (NAVAHCS, 1999).

All employees, students, and volunteers receive specific training about the confidentiality of health information and sign a confidentially agreement at the time of employment (The NAVAHCS Information Security Notification, 2001).

The NAVAHCS has a policy prohibiting the disclosure and sharing of passwords, access codes, and other user identification. Unique identification codes are used only to represent individual persons and are of sufficient length to permit NAVAHCS to issue a unique password for every user. The security administrator specifies a minimum password length that is enforced by the system. The system permits users to choose their own password without assistance or involvement by security administration and requests the user to select a password at initial sign-on and at timed expiration intervals. Users may change their password at will but it is prohibited to reuse them.

There is a policy that prohibits employees from loading unauthorized software into NAVAHCS' computers and from illegal reproduction or use of licensed computer software. The use of pirated or illegally obtained software is strictly prohibited. To ensure compliance with software copyright and licensing agreements, ISSL routinely conducts microcomputer audits. All new software is tested on a test computer to avoid damage to working computers if a virus is present. The test machine is set up for users permitting them to scan software acquired from outside sources. Users are given training which covers the risks that viruses pose to AIS assets, how viruses are introduced, how to prevent and detect them, warning signs of the most common viruses, and what to do if a virus is detected or suspected.

Contractors and vendors who provide services to NAVAHCS and who require access to PHI must sign security and confidentially agreements for themselves and for their employees and agents. Also, they must submit to a background investigation commensurate with the required level of access. This was discussed in detail under Business Associate Agreements in the Privacy section.

The NAVAHCS Information Security Officer (ISO) has the responsibility to conduct and monitor training of contracted employees in the use of the automated information systems and related applications. Any records created by a contractor in the course of treatment, payment, or healthcare operations are the property of NAVAHCS and are not to be accessed, released, transferred or destroyed except in accordance with applicable federal law and regulations. These agreements are covered under Patient Medical Records – VA Form (24VA136). When responding to a patient's request that copies of records be released to a third party, the contractor refers all patients to the NAVAHCS HIM officer for release of records. Since the records

generated are VA records, the contractor must retain the records for the same time period that NAVAHCS is required to retain the records, or the contractor must deliver them to NAVAHCS for retention. Penalties and liabilities are provided in the Privacy Act.

Physical Safeguards §142.308(b):

Both the Privacy Officer and the Information Security Officer routinely conduct rounds to assess physical controls. During the course of this research, I made physical safeguard rounds with the Privacy Officer (Sharon Chapman, Health Information Management). We toured the file room, the urgent care triage room, primary care, extended care and rehabilitation center (ECRC), and the Domiciliary building. The following security problems were found and are detailed by area or department.

File Room:

The file room is located in a physically secure area with signs that caution that only authorized personnel are allowed access. The file room/medical administration system record room door is locked.

Urgent Care:

In the urgent care center patients are triaged with the door open. The computer terminal is in view of passer-bys in the hallway.

Primary Care:

In primary care, the records were behind the desks but names were viewable to all patients checking in. The computer terminals were faced away from patients checking in and the fax machine was in a secure location. Patient records were kept in racks outside of exam rooms with no monitoring. Nurses conducting telephone triage were subject to unauthorized monitoring from anyone passing by.

Pharmacy:

A TelePrompTer in pharmacy is used to notify patients in the waiting room to pick up their medications. Providers were observed discussing diagnostic findings in the urgent care center in front of other patients.

Dental:

Curtains were not used by staff to block patient view into the dental area.

Nuclear Medicine:

X-rays were visible in nuclear medicine, and a workstation in the hallway showed both the x-ray and the names of patients in.

ICU, Medsurg (4A), Extended Care:

Patients were visible from the hallway with the door open. Names were outside of patient rooms in ICU, 4A, and in the extended care. In extended care, patient appointment boards with names were visible to everyone. Computer terminals are in the hallway in plain view. Charts with patient's names were in plain view. In the kinesiotherapy clinic the name board was in plain view.

Domiciliary:

In the domiciliary building he files are in a room out of sight but names are outside of patient rooms.

Compliance with physical security standards at NAVAHCS is better in some areas than in others. This facility has outlined excellent physical safeguards for protecting data integrity and confidentiality. There are definite assigned responsibilities for security, and formal policies and procedures address controls for access and the backup and storage of data. The Computer Security Act of 1987 requires mandatory, periodic training in computer security awareness for all individuals responsible for the

management, use, or operation of federal computer systems that process sensitive information. NAVAHCS is fully compliant with the educational elements of this directive.

Access to more sensitive areas is limited to protect equipment from vandalism and theft. Printers, copiers, and other items of equipment that have a relatively high potential risk of fire are placed in areas that have true floor-to-ceiling walls constructed of masonry or other fire-retardant material. Paper stock and other fuel sources are kept to a minimum, while cleaning solvents and other flammables are stored in a closed area. Data, software, documentation, and other assets are required to be protected from fire damage by fireproof storage containers and off-site storage to comply with the AIS security policy, but according to the information security officer there are no actual fireproof storage containers in use at NAVAHCS.

Physical access to the computer room is limited to authorized personnel. Entrance doors are closed unless they must be opened for equipment maintenance or for deliveries. Service line managers are responsible for ensuring that appropriate measures are taken to protect remote terminals and other peripheral equipment from misuse, theft, or unauthorized use (MCM NO.15-26, 2002).

Computer equipment is located in areas where the potential for flooding is low, and electrical and communication cables that pass through perimeter walls are in sealed conduits. Openings around water pipes and air ducts are also sealed, according to the Facilities Service Line Manager.

Microcomputers are protected from the electrical threats of spikes, surges and outages by spike and surge protection. Uninterrupted power supplies, diesel generators, and secondary power feeds from separate poser substations protect

mainframes for extended power outages. The transformers and motor generators also protect them from transient electrical events.

The VistA computer system supports disaster recovery procedures and in the event of a hardware/software failure, the system can recover to the point of the failure. The system supports disc mirroring or shadowing for security downtime processing and error recovery. It also provides sufficient back-up and recovery features to assure no data loss after a system failure (VHA OI, 1999). Essential information, including personal computer data files, business files, records, manuals, and office procedures, that will need to be restored following a disaster is identified in each service line's contingency plan. Backup copies of all identified files and records are stored in a secure location in a separate building.

No countermeasures are readily available to reduce the likelihood of a natural disaster, although the secondary effects such as electrical events, fires, and flooding are considered. Service line managers are responsible for keeping their employees informed of proper procedures for fire safety, removal of equipment from the premises, protection of equipment and information, and for reporting theft of NAVAHCS assets.

Effective housekeeping procedures are in place to minimize potential fire hazards that result from an excessive buildup of trash and the operational disruption that can occur due to dirt or dust accumulations on magnetic storage devices (MCM NO. 15-24, 2002).

All NAVAHCS employees are responsible for retrieving all printed outputs they request from printers. Documents that contain sensitive information or PHI are placed in 'sensitive' disposal bags for destruction or are shredded to protect the confidentiality of the data.

Inactive paper-based or computer based records are archived at NAVAHCS for three years before they are sent to the Federal Record Center for an additional 72 years. While archived, they are protected from loss, damage, and unauthorized disclosure through storage in a locked area.

All staff receives education about the elements of physical security, including the importance of confidentiality and information security in new employee orientation prior to accessing the VA system. This is reinforced in annual mandatory AIS security training. This education is in accordance with OPM Regulation 5 CFR Part 930, Training Requirement for the Computer Security Act. Staff is made aware of their security responsibilities and how to fulfill them. Users of information technology systems are apprised of the vulnerabilities of the system and the policies and goals for protecting data and information. They are trained in computer security practices for the protection of equipment, passwords, files, data, and magnetic storage media. Measures to update and backup data and files and protect against viruses and worms are posted electronically to inform all NAVAHCS employees.

The service line manager is responsible for ensuring that all employees comply with established procedures in service/support lines where fax machines are physically located, however a transmission log is not maintained. Health Information Department staffs are required to authorize faxing of all medical record information, and according to their statement, they feel that “99% of all protected health information comes through Release of Information (ROI)”. A cautionary statement is placed on all fax cover sheets stating that the fax is intended only for the use of the person or office to whom is addressed and may contain information that is privileged or confidential (MCM N0. 15-26, 2002). All incoming documents are monitored so they can be routed immediately in

a secure fashion. During rounds with the Privacy Officer, I noted that some fax machines were not under continuous observation, although they were all located in areas where patients and unauthorized personnel were not likely to be without supervision.

The NAVAHCS has a procedure in place to screen both federal and contract personnel who participate in the design, development, operation, or maintenance of sensitive applications and systems, as well as those who access sensitive data or information. The Director or designee is responsible for ensuring that all positions are reviewed and assigned a sensitivity level that is commensurate with the degree of supervision. The Director is also responsible for verifying the extent of security and protective measures in effect, the nature of the data being processed and the degree to which the data is accessible by individuals through outside terminals. The Director or designee monitors the extent to which the activities are performed in isolation and the degree of access to other data. VA Form 50 4236, Position Sensitivity Level Designation, is used to determine the appropriate designation.

The level of pre-employment clearance screening varies from a minimal check to a full background investigation, depending upon the sensitivity of the information to be handled and the magnitude of loss or harm that could be caused by an individual. All NAVAHCS positions are reviewed and assigned a sensitivity level commensurate with the degree of supervision necessary and the extent of security and protective measures in effect, as well as the nature of the data being processed and the degree of accessibility to other data in the system. Each employee's supervisor submits a new access request when the employee starts work. VA Form 50 4236, Certificate of Eligibility, is used to certify that an employee is determined eligible to occupy a position

designated as sensitive. A security officer within the Office of Inspector General (OIG) issues this form after a background investigation is conducted. When an employee transfers to a non-sensitive position or is separated from VA employment, the OIG Security Office should be notified so that the Certificate of Eligibility can be revoked (MCM No. 15-26, 2002). Personnel within NAVAHCS' human resources department stated that this is not routinely done. Although position descriptions should be, and often are, written to reflect specific security responsibilities and position sensitivity levels, this is not always confirmed on the OF8 (Optional Form 8 Position Description Sheet) (N. Campbell, personal communication, January 23, 2002).

When the user's status changes, the user's supervisor and the ISO review the user's current need to continue accessing menu options. (As an administrative resident I did not qualify to continue accessing the same clinical menus that I accessed as a nurse manager, and my menus were severely restricted). When an employee is terminated, the supervisor and ISO take action to ensure that the employee no longer has possession of or access to sensitive data and that the employee has returned all keys and access devices. Security codes and electronic signatures are reviewed for termination. The OIG Security Officer is notified if an employee leaves a position requiring a sensitivity level designation.

Technical Security Services §142.308(c):

There are security policies in place that partially address and describe record processing and electronic healthcare transactions. MCM NO. 15-26, "The Automated Information Systems (AIS) Security Policy", establishes the protocol and responsibility for information system security within the NAVAHCS. The program is designed to protect data from unauthorized access, disclosure, modification, destruction, or misuse.

The Medical Information Security Service (MISS) Program Office, part of the VHA Office of Information, provides oversight for the development and administration of security programs within the VHA. It develops and publishes security policy and guidelines and responds to information security incidents within VHA. It performs remote vulnerability studies on VHA information systems (VHA OI, 2000, August).

The information security officer and the ISSL Manager are responsible for the maintenance of electronic record systems and for ensuring that adequate software security measures are implemented. Anti-virus software is employed to help detect and block computer viruses and other forms of sabotage. Procedures for implementing this policy are found in VA handbook 6210, “Automated Information Systems Security”, and MCM NO.15-26, “Automated Information systems (AIS) Security Policy”.

The NAVAHCS has technology in place that ensures that only authorized entities gain access to network resources. The use of individual access and identity verification codes is mandated, and terminals that are routinely used to access health information have programmed “time-outs”. ISSL has the ability to positively identify authorized users of systems and remote terminals, authenticating an individual’s right to have access to specific data and preventing individuals from gaining access to programs for which they are not entitled (MCM N0. 15-26, 2002). The system allows for defining access to specific data elements, files, functions, menus, commands, and networks based on the user’s patient care responsibilities or position descriptions (VHA OI Technical Services, 2001). Veterans Health Information Software and Technology Application modules contain software security keys that control access to menu options and restricts access to only those that require it in order to perform their duties. This

provides NAVAHCS with a system of internal audits for monitoring compliance with security requirements (MCM NO.15-26, 2002).

When a file is created, the creator can stipulate that it be a “read”, “write”, or “delete”. The creator can have shared files within a service line or a group. Different segments of a patient record can be secured individually; this is built into the computerized patient record system (CPRS). Patient information leaving the facility is supposed to be encrypted through VistA, but this is not always enforced (J. Orey, personal communication, March 5, 2002). A VA confidentially strategy and the establishment of the VHA Encryption Working Group were proposed in 2001. On July 20, 2001, a group of VHA field personnel, OI staff, and others met with representatives from the VA Cyber Security Office, Veterans Benefits Administration, and the National Cemetery Association to get agreement on a strategy. The group reached a tentative agreement but a review of it has not been completed. Once finalized, an enterprise-wide implementation plan will be developed (VHA Transition Paper, 2001).

E-mail that contains sensitive or confidential information is protected from unauthorized access, alteration, or disclosure by encryption through a public key infrastructure. This is available on a very select basis however due to cost. Ordinary e-mail can be sent as “confidential” or as “information only” and if that is done, it cannot be altered or forwarded. The system supports the encryption of the password file or the password information. Patient related transmissions and files sent to remote locations within VHA are not encrypted. Community based outpatient clinics are considered to be within our system and have a dedicated data communication line.

Procedures are in place to document the receipt and transmission of electronic records using the Remote Data View software package, and in other stations the

Network Health Exchange software package. Healthcare providers within the VISN routinely request health information and data from remote sites. These messages are tracked, and it is possible to go back and check who sent and who read a specific transaction.

The ISSL has an audit mechanism and a policy (AIS Security Policy) that records and examines system activity. Security keys within the patient-sensitivity function of the information management system software, control access to restricted records. Each time a record is accessed, the system logs the patient name, user name, date/time of access, and the option used to access the record. The sensitive record access log is monitored by the ISO. Audit trails provide a chronological record of system activities that enable reconstruction, review, and examination of the sequence of activities of each event in a transaction. Audit trails can be produced to detect and identify unauthorized access, including user identification codes and invalid passwords with date, time, and location. All modifications to security settings and parameters can be audited via FileMan (an application within VistA that can create and access data files). The records generated from these audits can be utilized to grant, modify or terminate privileges (VHA OI, 1999).

When NAVAHCS proposes to adopt new technology, the Information Systems service line manager reviews all activities and puts together an IT plan and a budget. The service line manager and ISO assess the potential for risk and make purchase decisions which then go before the resources committee for appraisal and final decision. Although policies are updated when new technology is adopted, it is not always as timely as it should be (J. Orey, personal communication, January 23, 2001).

Employees are notified of all policy changes by messages on VistA, Outlook Exchange, and the NAVAHCS Intranet web page.

Technical Security Mechanisms §142.308(d):

Technical security incorporates equipment, components, devices, and associated documentation that pertain to the security of automated information systems and telecommunications.

The NAVAHCS has not created a network diagram, which includes the location of remote access points (Internet Gateways), and the number of remote users or remote locations. This facility does not have its own Internet gateway, but the system is protected from unauthorized access via the Internet through the use of firewalls, cryptography, and authentication devices. Authorized staff at the VISN level review firewall logs, intrusion detection alerts, and other data sources to identify potential security breaches. Security devices are routinely patched when it is discovered that a VistA program doesn't work under certain conditions or after prior modifications. MISS may issue alerts with instructions about vendor sources and installation instructions for a specific patch.

Non-essential services on servers are disengaged when ISSL personnel are notified by MISS that they pose a potential security threat. Intrusion detection systems to monitor traffic through access points are maintained by the VISN office. In the event of suspicious network activity the system automatically detects and sends a message to the VISN Chief Information Officer (CIO). It is at the VISN level that firewall logs, intrusion detection alerts, and other data sources that identify potential security breaches are maintained (VHA OI 2001). In the January 9, 2002 minutes of the Business Operations Executive Board of VISN 18, firewall and virtual private networks

were discussed (VISN 18, 2002). It was stated that additional firewalls and virtual private networks are necessary, as additional business partners require connection to our network or to equipment within our network. Firewall and virtual private network protection are part of new security requirements, and the VISN has installed three firewalls this year. A recurring, mandated budget requirement is the Penetrations Studies Initiative which involves a contractor attempting penetration to find security breaches within the network (VISN 18, 2002). The ISO and ISSL manager routinely report and document any instances of suspicious activity and security device malfunctions to the VISN and to MISS, although the VISN is usually aware of questionable activities and malfunctions first. The ISSL manager submits a weekly report to MISS on local incidents.

The NAVAHCS attempts to ensure that all security devices are upgraded promptly and configured optimally. The Information Security Officer monitors this duty and the VISN security updates patches and other network security services.

The ISSL manager is responsible for ensuring that adequate software security measures are implemented and that all information resource sharing agreements pertaining to computer hardware and software are reviewed for security issues. All software packages installed on NAVAHCS computers are registered with the ISSL who documents purchase receipts and ensures compliance with copyright and licensing agreements (MCM NO.15-26, 2002).

Healthcare came relatively late in the deployment of computer technology and this has placed the industry in a difficult position. The challenge of upgrading information systems reaches beyond acquiring new software. HIPAA legislation is a landmark development because it is forcing the healthcare industry to move forward in

information utilization and security (Fuller, 1999). Compliance will require more organizational initiatives than technical features and NAVAHCS appears to be well situated to move forward with confidence.

Navigating Towards HIPAA Compliance

The scope of HIPAA privacy regulation is founded on the premise that health information should be easy to use for healthcare purposes and very difficult to use for any other purpose. While HIPAA does not require a specific privacy compliance plan, it does mandate the creation of policies and procedures that are wisely and comprehensively designed. The "key" to compliance with the privacy rule resides in the quality of documentation. The common phrase among healthcare personnel is "if it's not documented, it wasn't done."

The final rule and the preamble use the term "reasonable" 256 times to describe the manner in which the rule is to be implemented by the various models of covered entities (Amatayakul, 2001). This presupposes some subjectivity for the interpretation of the term "reasonable". What is reasonable for one entity may be unreasonable for another. The intent of the rule is to allow each entity to determine this for themselves. It will be necessary to place compliance activities on a continuum between doing too much and too little. Excessive attention to privacy can impede many of the goals of a health care system.

In preparation for implementation, the current procedures for the use and disclosure of health information at NAVAHCS were compared with the proposed privacy and security standards to determine readiness. NAVAHCS is partially compliant in those areas already covered by the Privacy Act, the Computer Security Act, and the Freedom of Information Act. These federal statutes were intended to be fair with regard

to the collection, use, or dissemination of patient records, although they fail to address the new challenges to individual privacy which have arisen from the automation of medical records. Collectively they represent an incomplete patchwork effort to address the privacy and security concerns of individuals regarding their protected health information (Gostin & Hodge, 2001). Still, these federal statutes are meaningful and confer valuable protection to health information in this facility. NAVAHCS and other governmental systems have an excellent foundation in place for meeting HIPAA compliance. In addition, the Medical Center Memorandums provide general policy coverage for many of the privacy and security standards of the final rule.

The following represent a checklist of policies to be addressed by NAVAHCS as it moves toward compliance.

Policy Checklist

Minimum necessary use and disclosure: A classification of persons, categorization of information and applicable conditions under which PHI may be disclosed is required. This may be manifested in a database with assignment of access authorization for paper and electronic information. This will describe routine/recurring circumstances and criteria to limit disclosure and recommend periodic audits.

Consent: This form should comply with the very specific requirements in the rule, and signed consent forms should be retained. Currently, there is a proposed modification from HHS that may remove the consent requirement and substitute an acknowledgment of receipt of the facility's notice of privacy rights and practices (HHS Fact Sheet, 2002).

Authorization: These are specific requirements for general authorizations as well as those for specific types of disclosures.

Complaints: Formally established policy, procedures, and office for receipt and disposition of complaints must be in place.

Sanctions: Confidentiality agreements that indicate personnel may be terminated for breaches of termination should be established and disseminated.

Whistleblower protections: Human resources will need a policy that includes how to file complaints and when to use PHI in the course of filing the complaint. Whistleblower protection already exists but will need to be HIPAA specific. DVA human resources management will review current Whistleblower policies, update them as appropriate, and disseminate revised policies this year (VHA OI HIPAA Workgroup, 2000).

Notice of Privacy Practices: This will be an extensive document that includes specific content requirements and will document the provision of the notice and all revisions. VHA will provide a standardized document to all facilities.

Training and education: Generic privacy training for all VHA employees will be developed to meet HIPAA requirements, with in-depth position specific training to be developed for implementation after the initial training. Attendance at initial and annual training will be documented. Employee Educational Systems will develop and provide the privacy training. A directive issued by the Office of the Under Secretary for Health indicating that privacy training is mandatory is said to be forthcoming (OI HIPAA Workgroup, 2001).

Safeguards: These refer to the proposed security rule and the requirement to adopt administrative, technical, and physical safeguards to protect privacy.

Rights to request restrictions: Policies on disclosures, access, amendment, and accounting for disclosures, including procedures and documentation process for carrying out these requests shall be clearly stated.

Use and disclosure without authorization: For facility directories and involvement in care, (i.e. family members, clergy), individuals must be informed and given the opportunity to object, and while documentation is not required, it would be wise to at least document the communication.

Research: Where an institutional review board has approved alteration or waiver of authorization, the alteration and waiver must be documented.

Business associate agreements: Contracting policies will be addressed at a national level with dissemination of guidance to the medical centers. Existing contracts should be checked to determine that they establish permitted and required uses and disclosures and safeguard information. There should be clear documentation of those direct associates who have access to PHI and the indirect agents of those associates. Their compliance with the contracting policy will need to be documented.

Mitigation of harmful effects of a use or disclosure: Establish a tracking mechanism and procedure for action (Amatayakul, 2001; Barlament, 2001; Gostin, 2000; Fuller, 1999).

Recommendations

1. Form a HIPAA Workgroup (task force) for NAVAHCS to monitor the implementation of VHA and VISN recommendations.
2. Coordinate privacy activities with security activities within NAVAHCS, recognizing that an overlap exists between these activities.
3. Identity current uses of individually identifiable health information which, under HIPAA, will be outside of the scope of permissible use without specific authorization.
4. Decide upon an appropriate policy that identifies information that will be subject to protection.

5. Develop methods for disclosing only the minimum amount of protected information necessary to accomplish any intended purpose.
6. Determine when and how identifiers will be removed from information in order to afford further protection.
7. Revise (create) an authorization form for release of information for all purposes other than treatment, payment, and healthcare operations.
8. Develop a consent form. Draft (VHA will provide this to all VISN's) a *Notice of Privacy Practices* that states the uses and disclosures that NAVAHCS intends to make with PHI. Any use not included becomes unlawful. Our providers must give this notice to each patient at the first service after the effective date of the rule and must also post a copy of the notice. We should provide the notice at enrollment and at least every three years after. Any modifications made will also have to be distributed. NAVAHCS will need to have written acknowledgment that patients have received and read the privacy notice. The NAVAHCS workgroup should think about how future revisions to the *Notice* will be communicated. HIPAA requires that a covered entity include in its *Notice* how any future revisions will be communicated. The Workgroup will decide how to best disseminate and track the distribution of the *Notice.*
9. Ensure that patients have a means to lodge complaints about the new information practices and about possible violations of privacy. The process that NAVAHCS establishes for handling complaints should be tracked from point of receipt through resolution with communication to the initiator of the complaint. (NAVAHCS needs to be aware of the patient option to register complaints with the HHS Office of Civil Rights).

10. Develop a mechanism for to account for all disclosures of PHI for purposes other than treatment, payment, and health care operations.
11. Develop (expand upon) a privacy training program for employees and volunteers about the requirements of the privacy rule under HIPAA. Incorporate this into new employee orientation as well. The VHA will probably issue guidance on program content. The NAVAHCS has already made a good beginning by having the Privacy Officer and Information Security Officer speak at new employee orientation.
12. Develop a mechanism for disseminating ongoing information privacy awareness reminders and updates within NAVAHCS. (The information systems service line can do this electronically)
13. Have Human Resources develop a system of sanctions for employees, ranging from retraining to reprimand to termination, for employees who are in violation of NAVAHCS' new privacy policies.
14. Revise contracts with business associates. (VHA will provide guidance). It will be necessary to obtain "satisfactory assurance" that each business partner will appropriately safeguard information. Under the draft as written now, NAVAHCS would also have to take "reasonable steps" to assure compliance in our associates. If this could change then, our obligation might be limited to appropriate confidentially clauses and a requirement to report only those inappropriate disclosures that are known.
15. Determine if it is possible to modify existing confidentiality agreements with third party electronic recipients of PHI.
16. A chain of trust agreement should be instituted between NAVAHCS and those third parties with which electronic health information is exchanged to ensure that the

same level of security will be maintained. NAVAHCS will need to ensure ongoing compliance monitoring of all agreements to see that privacy issues are being addressed and that business associates and subcontractors are compliant with the privacy standards. The legal office and the contracting officer will need to identify all parties to be included in chain of trust agreements.

It is expected that the VHA Office of Information will update all VHA policies, directives, and manuals relating to privacy, individual's rights, and release of information to comply with the final privacy rule requirements, but it is important for NAVAHCS to be familiar with the areas that will be addressed. The Office of Information will also examine conflicts between the Privacy Act of 1974 and the final privacy rule and will issue guidance on the resolution of any conflicts in policy (VHA OI Workgroup, 2001, July; Hjort, 2001).

Security

As with many of the privacy standards, implementation of HIPAA security standards will involve a reengineering of business practices. The development of information technology software will no doubt play a significant role in VHA and NAVAHCS' efforts to become HIPAA compliant, but changes in business methods and organizational culture will also be critical to successful compliance.

Implementing the proposed security rule is less difficult for VHA and NAVAHCS because of the existing security implications required to comply with the Privacy Act of 1974 and the Computer Security Act of 1987 (Department of Veterans Affairs, 2001, November). NAVAHCS has been following the established Information Security program of the VHA's Medical Information Security Service. The Information Security

Officer and ISSL currently have an excellent security training awareness curriculum and many policies and procedures in place.

Recommendations

Administrative Security:

1. Design, implement, and document technical audit capabilities for all systems. To assess system activity and potential security incidents, a periodic audit should be conducted of all the organizational systems which process health information. Documentation requires records and logs that demonstrate routine and thorough audits. (Guidance will probably come from the VISN).
2. Enforce compliance with all VHA policies at this level. Information Security Officer should review these to ensure compliance and continuity.
3. Review employee position descriptions and security profiles for completeness.
4. Verify that termination procedures are consistently applied for all users.

Physical Security:

1. Ensure that periodic reminders are provided to service line managers and all employees about physical security safeguards, i.e., computer terminals, workstation use, locked rooms, charts vulnerable to unauthorized viewing, privacy screens/curtains, conversations, etc.
2. Improve documentation of maintenance records of locks, walls, and doors that allow access to areas requiring physical access control.
3. Have all service line managers ensure that paper records are stored under lock and key, and returned to their place, particularly during weekend, holiday, evening, and night tours.

4. Charts should never be left in exam rooms when other patients are waiting for their appointments.
5. Enforce the current physical access control policies and document when formal access reviews and rounds are accomplished.
6. All clinics, offices, and laboratories should consider keeping sign in sheets behind the reception desk.

Technical Security:

1. Enforce implementation of user access or authorization based on minimal need to know.
2. Budget resources (FY03) for new technologies that will allow for the protection and security of patient identifiable data.
3. Require and review complete documentation for security alarms.

Conclusion

At the outset of this project it was apparent that the size and scope of HIPAA would make any analysis of compliance with its regulations daunting. The voluminous nature of the Act (over 1200 pages) requires that limitations must be imposed on any single attempt at understanding its application. This project developed a gap analysis/risk assessment for compliance issues regarding only privacy and security at NAVAHCS.

A review of the Act and supporting literature provided the basis to begin this task. Examination of documents and policies, interviews with personnel, and on-site investigations were conducted throughout the facility. This investigation revealed areas of compliance and non-compliance with regard to privacy and resulted in specific recommendations to be addressed by a future NAVAHCS Workgroup. Inspection of

security standards also disclosed areas that were not in accordance with the HIPAA requirements. Recommendations were developed based on the identified gaps. These are not intended to be a means of bringing NAVAHCS into compliance. Rather, they are intended to provide a basis for dealing with these discrepancies proactively.

A common perception within the healthcare industry is that legislation or rules which have not been enacted, or are to become operational at some later date, should be viewed as suggestions or possibilities only. What is written today can be rewritten or rescinded tomorrow. The recent proposals regarding consent lend some credibility to this belief. HHS just announced a proposed change to the privacy rule on March 21, 2002. HHS may eliminate the requirement that patients sign a written consent for routine uses of their medical information. Providers may not need to receive prior consent for treatment, payment, or health care operations. Instead the proposal requires providers to ask patients to acknowledge their privacy notices, but allows them to treat patients even if they do not (HHS Fact Sheet, 2002).

It is also difficult for organizations to justify the allocation of scarce resources to anything that has a tentative future compliance date. For these reasons it is understandable why many are taking a wait and see position hoping for the best.

The hope that HIPAA will go away or be rescinded is not a proactive approach to dealing with it. HIPAA has taken center stage when it comes to privacy and security. Clearly, the new rules will require health care providers to make significant changes in the way business is conducted. Even though HIPAA standards are still being finalized healthcare organizations must move quickly to develop and implement a compliance plan.

These standards have the potential to completely restructure the VHA privacy program and initiate the most substantially inclusive changes to privacy practices in VHA history since the enactment of the Privacy Act of 1974 (Putt, 2001). Some aspects of HIPAA compliance will call for a ONE VA solution, i.e., a single solution coordinated across all VHA, VISNs, and medical facilities (Office of Information HIPAA Coordinator, 2000). NAVAHCS, as part of the vast VHA health care architecture, will need to implement new policies, provide training to all employees, and balance itself between HIPAA and other federal privacy laws.

The scope of involvement is all-inclusive and will affect every aspect of the way work is conducted throughout the facility. The majority of administrative and technical solutions for compliance will come directly from VHA Central Office and the Office of Information HIPAA Workgroup. Some security measures will be national initiatives and many policies will be issued through national directives and manuals. This project is intended to familiarize senior leadership at NAVAHCS with HIPAA, the HHS standards, and efforts currently underway within the DVA.

Although NAVAHCS will need to make some changes in its infrastructure, (workspaces and information technology), most of the effort will be focused on revisiting and updating policies and procedures, and this will naturally lead to the need to inform and educate staff on the new way of doing things. The majority of HIPAA readiness tasks will be people related.

Considering the breadth of the changes required and the number of systems and departments potentially affected by the requirements, administrators must use the time wisely. Now is the time to begin the development of specific policies and procedures that will remediate the weaknesses found in this assessment.

Privacy and security are fundamental necessities for healthcare providers. These issues must be addressed and dealt with in a manner intended to provide the highest quality care possible. This project provides an insight into the current privacy and security status at NAVAHCS. By discovering gaps in compliance between the existing policies and practices and those required by HIPAA important information has been developed which may provide a useful tool for a future taskforce.

Organizational and strategic management must be adaptive. To this end, being prepared for anticipated change is an advantage. By understanding existing deficiencies as we move toward change, our efforts to accomplish change can be made more efficient. It is hoped that this project will help in this regard by identifying the gaps that need to be closed to achieve HIPAA compliance.

Appendix A

Glossary

Access:
The ability to enter automated information systems. The permission granted to users and controlled by a set of procedures performed by hardware, software, and administrators.

Authorization:
Document obtained by a covered entity in accordance with 45 CFR §164.508 in order to use or disclose PHI for a purpose other than treatment, payment or health care operations.

Business Associates:
A person or company that performs an activity for a covered entity that involves the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, and benefit management.

Chain of Trust Partner Agreement:
A chain of trust agreement is a contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged.

Consent Form:
Document obtained by a health care provider in accordance with 45 CFR §164.506 in order to use or disclose an individual's PHI for treatment, payment or health care operations. A consent form is to be obtained one time from the individual and will remain in effect until in is revoked in writing.

Covered Entities:
Any organization that is a health plan, a health care clearinghouse, or a health care provider that transmits health information electronically in connection with a standard transaction.

Disclosure:
The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Health Care Clearinghouse:
A public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.

Health Care Operations:
Activities such as quality assessment and improvement, case management and care coordination, conduct of training programs, accreditation, certification, licensing, credentialing, auditing, underwriting and premium rating, and other administrative activities.

Health Care Provider:
A provider of services, a provider of medical or other health services, and any other person or organization who furnished bills, or is paid for health care services or supplies in the normal course of business.

Health Information:
Any information, oral or recorded in any form or medium, that is created or received by a health care provider, health plan, employer, life insurer, school, or health care clearinghouse; and relates to the past present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Health Plan:
An individual or group plan that provides or pays the cost of medical care, including the veterans health care program under 38 U.S.C. chapter 17.

Hybrid Entity:
An organization that is a covered entity whose primary function is not as a health care provider, health care plan, or health care clearinghouse. The “health care component” of the organization must comply with the Privacy Standards.

Individually Identifiable Health Information:
Any information including demographic information collected from an individual, that is created or received by a health care provider, plan, employer, or health care clearinghouse, and relates to the past, present, or future physical or mental health of an individual, the provision of care to an individual, and identifies the individual.

Notice of Privacy Practices:
A formal notice defined by the organization that serves as a public indicator of the organization’s policies and procedures related to the use and disclosure of PHI.

Payment:
Billing, collection, obtaining premiums, determining eligibility, coordination of benefits, medical necessity or utilization review, etc.

Provider:
Any person or organization that furnishes, bills or is paid for, health care services or supplies in the normal course of business.

Protected Health Information (PHI):
Individually identifiable health information that is transmitted or maintained in any form or medium including but not limited to paper and electronic.

Sensitive Information:
That data contained in an automated information system that must be protected from accidental or intentional, but unauthorized disclosure, modification, or destruction due to its personal or mission criticality.

Transaction:
The transmission of information between two parties to carry out financial or administrative activities related to health care.

Treatment:
The provision, coordination, and management of health care and related services.

VistA:
Veterans Health Information Systems and Technology Architecture. VistA is build on a client-server architecture which ties together workstations and personal computers with graphical user interface at VHA facilities, as well as software developed by local medical facility staff. VistA also includes the links that allow commercial off-the-shelf software and products to be used with existing and future technology.

(Bogen, 2001; Medical Information Security Service, 2000; Office of Information Workgroup, 2001)

Appendix B

VHA Office of Information (OI) HIPAA Workgroup Ranking Criteria

Ranking Scale:

0 – No identified process or control
1 – Informal or partial process or control
2 – Process or controls implemented for many required HIPAA elements
3 – Process or controls fully implemented for all required HIPAA elements
4 – Process or controls exceed required HIPAA elements

HIPAA Requirement	Ranking	Risk Area	Concern
45 CFR Parts 160 & 164	2	Privacy Officer, employee code of behavior, misc.	NAVAHCS will need to more strictly limit access to and use of PHI to need to know only. "Minimum Necessary" will need to be enforced.
Consent: §164.506	1	*Notice of Privacy Practices*	NAVAHCS does not have this but VHA will coordinate the drafting. VHA Form 1010EZ does not cover use and disclosure for treatment, HC operations, and business practices. VHA will revise to comply with HIPAA.
Authorization §164.508	1	"Authorization" is different from consent and needs more details. May not condition TPO on the individual's authorization to use or disclose information.	No specific authorization form. Psychotherapy notes not separate from other PHI.
Right of Access and Amendment §164.524and §164.526	2	Compliant in the most important areas. Timelines more stringent.	No policies to address amending records received by other covered entities.
Administrative requirements: §164.530a	2	Privacy and security officer in place	
§164.530b	2	Training and education	Need a formalized, current, ongoing program. EES, OI will develop a program for all employees, students, volunteers and contractors.
§164.530c	3	Safeguards to protect PHI	Privacy policies in place but actual security needs to be tested.
§164.530d	3	Formal policy and office for receipt and disposition of complaints	NAVAHCS responds to complaints through HIM but needs to develop a policy. OI will establish a formal process.
Use and Disclosure for which consent is not required §164.5129c	3	Public health, law enforcement agencies	Privacy Act preempts HIPAA in some areas and is more stringent. Need a strong policy to address data elements that can be released.

Business Associates: 45CFR §§160.103, 164.502(e), 164.514(e)	2	Establishes standards that will ensure that the use and disclosure of PHI by a covered entity's business associate is appropriately protected.	Need to track, evaluate and update contracts. No current procedures to ensure compliance or a process to enforce compliance. VHA will provide guidance and disseminate generic language for contracts. VHA will institute MOU with VA components that are business associates.
Use and disclosure for involvement in the individual's care and notification purposes:	1	Formal policy that will allow a patient to request that disclosure of PHI be restricted.	NAVAHCS needs a written protocol to inform patients on admission of disclosure of PHI to family members.
Other Requirements	2	Facility Directory	NAVAHCS does not maintain a facility directory. A process to allow vets to opt-out needs to be determined by VHA.
Security §142.308	2	Administrative procedures: contingency plan, information access, audits, personnel, training	Inconsistently documented audits and reviews.
Security §142.308(b)	2	Physical privacy safeguards	Terminals need to be out of view. Curtains not used consistently, names and appointment boards and charts in plain view. Charts may be left in exam rooms.
Security §142.308(b)	2	Physical security, cont.	No fireproof storage containers for data, software, other documentation. PD's not consistently written to reflect sensitivity levels and not always confirmed by HR.
Security §142.308(b)	2	Physical access controls	Documentation of testing inconsistent.
Security §142.308(c)	2	Authorization control	Inconsistent implementation of access based on minimal need to know. (Role based, user based, context based). Some menus provide additional access inappropriate to the role of the user. This will need to be defined as well, especially for Quality Programs.
Technical Security §142.308(c)(d)	2	Audit control	Not all systems have audit capabilities implemented with respect to risk. Audit logs not always reviewed and documented in a timely manner.

References

AAMC - Association of American Medical Colleges. (2001). Guidelines for academic medical centers on security and privacy practical strategies for addressing the health insurance portability and accountability act (HIPAA). Retrieved October 18, 2001, from the http://aamc.org/members/gir/gasp

AHIMA Policy and Government Relations Team. (2001a). Final rule for standards for privacy of individually identifiable health information - what the rule covers. Retrieved September 19, 2001, from http://www.ahima.org/dc/privacy.rule.7.html

AHIMA Policy and Government Relations Team. (2001b). Preemption of state [and other] law[s]. Retrieved September 19, 2001, from http://www.ahima.org/dc/privacy.rule.3.html

Amatayakul, M. (2001). *HIPAA on the job: Documenting your compliance with HIPAA's privacy rule.* Retrieved October 3,2001, from http://www.ahima.org/journal/feature.0104.3html

Amatayakul, M. (2000, April). Getting ready for HIPAA privacy rules. Retrieved September 24, 2001, from http://www.ahima.org/journal/features/feature.0004.5.html

American Civil Liberties Union. (2001). Privacy Rights -Introduction: American civil liberties union freedom network. Retrieved August 31, 2001, from http://www.aclu.org/issues/privacy/isprivacy.html

American Hospital Association. (2001a). HIPAA standards: High points of the guidance for hospitals. Retrieved September 18, 2001, from http://www.aha.org/hipaa/resources/HhsGuidanceB0706.asp

American Hospital Association. (2001b). *The one-year extension for complying with HIPAA's standards for electronic transactions: How does it affect you?* Retrieved Jan 3, 2002, from http://www.aha.org/hipaa/resources/electransactextention.asp

American Hospital Association. (2001,September). Legal advisory: State law preemption under HIPAA (Issue Brief No. 12:48). Chicago, Ill: Author

American Medical Association. (2001). Health care regulation HIPAA headaches. Retrieved September 18, 2001, from http://www.ama-assn.org/ama/pub/article/3216-4806.html

Apple, G. & Brandt, M. (2001). Ready, set, access! An action plan for conducting a HIPAA privacy risk assessment. *Journal of AHIMA,* 72*(*6), 26-32.

Barlament, J. (2001). The impact of HIPAA's privacy rules on multiemployer group health plans. *Employee Benefits Journal,* 1, 1-6. Retrieved January 2, 2002, from insurancenewsnet.co.uk./article.asp

Beacon Partners. (2001). Guide to understanding and complying with HIPAA security and privacy regulations (2nd Ed.) [Brochure]. Norwell, MA: Author.

Beauchamp, T., & Childress, J. (1994). Professional - Patient Relationships. In (Ed.), *Principles of biomedical ethics: 4th ed.* (p. 407). New York: Oxford University Press.

BENEFITS next. (2001). HIPAA Final Privacy Rules. Retrieved July 24, 2001, from http://www.benefitsnext.com/content/view.cfm?articles_id=2467&subs_id=6

Bengani, P. (1997). Privacy in the digital age. Retrieved September 4, 2001, from http://is.gseis.ucla.edu/impact/s9/Focus/Commerce/privacy/privacy.html

Bogen, J. (2001). HIPAA challenges for information security: Are you prepared?. Retrieved January 22, 2002, from http://www.HealthCIO.com

Braithwaite, B. (2001, July). Guidance on Final Privacy Rule. Retrieved July 9, 2001, from http://HIPAA-REGS@LIST.NIH.GOV

Brandt, M., Carpenter, J. (2000). Practice brief: Information security: A checklist for healthcare professionals. Retrieved September 18, 2001, from http://www.ahima.org/journal/pb/00.01html

Bricker & Eckler. (2001). HIPAA privacy joint information center. Retrieved October 1, 2001, from http://www.bricker.com/hipaa/display/print/list.asp

Burks, C. & Collins, S. (2001). Executive summary results by regulation. Health Insurance Portability and Accountability Act (HIPAA) security assessment executive summary (VHA Publications). Washington, DC: U.S. Department of Veterans Affairs

Cap Gemini Ernst & Young. (2001). The Health Insurance Portability & Accountability Act. Retrieved September 24, 2001, from http://www.mcareol.com/hfmafree/arttcl823.pdf

Cassidy, B. (2000,June (a)). HIPAA on the job: Enhance your organization's awareness of HIPAA. Retrieved September 24, 2001, from http://www.ahima.org/journal/features/feature.0006.4.html

Cassidy, B. (2000, April (b)). HIPAA: Understanding the requirements. Retrieved October 3, 2001, http://www.ahima.org/journal/features/feature.0004.3html

Center For Democracy & Technology. (2000, September). Medical records privacy. Retrieved September 12, 2001, from http://www.cdt.org/privacy/medical/

Computer Based Patient Record Initiative (CPRI). (2001). *CPRI Toolkit: Managing information security in health care (3rd ed.)* [Brochure]. Bethesda, MD: Author.

Davidson, Dick. (2001). *AHA HIPAA standards - resources - MOU.* Retrieved October 18, 2001, from http://www.aha.org/hipaa/resources/LtrBushThomasB0523.asp

Dennis, J. (2000). Privacy and confidentiality of health information. San Francisco: Jossey-Bass.

Department of Labor, Health and Human Services, and Education, and related agencies. (2001). Appropriations Bill, 2002, Report (Report No. 107-229). Washington, DC: US Government Printing Office.

Department of Veterans Affairs. (January 30, 1997). VA Directive 6210. *Automated information systems security*. (Department of Veterans Affairs publication). Washington, DC: Author.

Department of Veterans Affairs. (2001, September 6). Health Insurance Portability and Accountability Act (HIPAA) Privacy Assessment Executive Summary. (Department of Veterans Affairs publication). Washington, DC: Author.

Department of Veterans Affairs. (2001, November 4). Health Insurance Portability and Accountability Act (HIPAA) Security Assessment Executive Summary. (Department of Veterans Affairs publication). Washington, DC: Author.

ERiskSecurity. (2001). HIPAA legal history. Retrieved September 12, 2001, from http://www.hipaacompliancecentral.com/history.html

Friedman, E. (2001). Who should have access to your information? Privacy through the ethics lens. Retrieved September 24, 2001, from http://www.ahima.org/journal/features/feature.0103.3html

Fuller, S. (1999, October). Implementing HIPAA security standards - are you ready? Retrieved October 2, 2001, from http://www.ahima.org/journal/features/feature.9910.1.html

GAO Testimony (September 8, 2000). VA information systems: Computer security weaknesses persist at the veterans health administration (Letter Report, 9/8/2000, GAO/AIMD-00-232). Retrieved October 3, 2001, from http://www.privacysecuritynetwork.com/Library/docs/GAO%20report%20on%20VA%2Ehtm

Goldman, J. (2000, December). Landmark health privacy law issued by Clinton administration. Retrieved September 12, 2001, from http://www.healthprivacy.org/info-url_nocat_show.htm

Gostin, L. (2000). National health information privacy - Regulations under the health insurance portability and accountability act. Retrieved July 30, 2001, from the World Wide Web: http://www.hipaacomply.com/legal.htm

Gostin, L., Hodge, J. (2001). Model state public health privacy project: Privacy and security of public health information. Retrieved November 27, 2001, from http://www.critpath.org/msphpa/ncshdoc.htm

Gradle,B. (2002). Business associates: A HIPAA compliance challenge. *Healthcare Financial Management,* 56(2), 23-27.

Gue, D. (2001). HIPAA regs - the HIPAA security rule (NPRM): overview. Retrieved October 4, 2001, from http://www.hipaadvisory.com/regs/securityoverview.htm

Hagland, M. (2001). The journey of 1,000 miles: Are providers really ready for HIPAA's privacy requirements? Retrieved September 18, 2001, from http://www.ahima.org/journal/features/feature.0102.3.htm

Harrington, S. (2001). HIPAA, hipaa, hurrah! A chance to achieve efficiencies sooner rather than later. *Health Management Technology,* 22(4), 2. Retrieved September 18, 2001, from http://www.healthmgttech.com/archives/

Health Information Compliance Insider: A Plain-English Guide to HIPAA Privacy & Security Regulations. (2001). What you should know about the new guidance on HIPAA privacy regs [Brochure]. New York: Author.

Health Privacy Project - Institute for Health Care Research and Policy. (2000). The 1996 health insurance portability and accountability act. Retrieved September 10, 2001, from http://www.healthprivacy.org

Health Privacy Project. (2000, December). Landmark health privacy law issued by Clinton administration. Retrieved September 12, 2001, from http://www.healthprivacy.org/info-url_nocat2303/info-url_nocat_show.htm

Health privacy regulation enhances protection of patient records but raises practical concerns: Hearings before the Committee on Health, Education, Labor, and Pensions, of the U.S. Senate. (February 8, 2001) (Testimony of Leslie Aronovitz, Director Health Care – Program Administration and Integrity Issues, of the General Accounting Office, GAO)

HHS Fact Sheet. (2001, May 9). Protecting the privacy of patients' health information. Retrieved July 10, 2001, from http://www.hhs.gov/news/press/2001pres/01fsprivacy.html

HHS Fact Sheet (2002). Standards for privacy of individually identifiable health information - Proposed rule modification. Retrieved March 25, 2002, from http://www.hhs.gov/news/press/20020321.html

HHS News. (1999, Oct. 29). HHS proposes first-ever national standards to protect patients' personal medical records. Retrieved September 10, 2001, from http://aspe.hhs.gov/admnsimp/nprm/press4.htm

HHS News. (2001, April 13). Statement by HHS secretary Tommy G. Thompson regarding the patient privacy rule. Retrieved July 10, 2001, from http:www.hhs.gov/news/pres/20010412.html

Higgins, M. (2000, December). Securing the perimeter - Strategies to secure remote access points to healthcare networks. Retrieved October 3, 2001, from http://healthmgttech.com/archives/

Hughes, G. (2001). Practice brief: Patient access and amendment to health records. *Journal of Ahima, 72(5)*, 1-8. Retrieved September 18, 2001, from http://www.ahima/journal/pb/01.05.4.htm

Institute for Health Care Research and Policy, Georgetown University. (1999, July). The state of health privacy: An uneven terrain. Retrieved September 10, 2001, from http://www.healthprivacy.org

Johns Hopkins Hospital. (2000, January 12). Draft HIPAA Security Summit Guidelines, Version1.1. *Paper from symposium held October 11-13, 1999. Revised January 12, 2000*. (Johns Hopkins publication). Baltimore MD: Author.

Joint Healthcare Information Technology Alliance (JHITA). (2000). A brief summary of proposed federal privacy regulation. Retrieved September 12, 2001, from http://www.jhita.org/hipprs.htm

Journal. (2001). Lawsuit against HIPAA privacy regulations. *Health Information Compliance Alert,* 1, 73-82.

Kammer, R. (2000, March 30). Statement of Raymond G. Kammer director national institute of standards and technology - technology administration U.S. department of commerce before the subcommittee on technology committee on science U.S. house of representatives. Retrieved September 19, 2001, from http://csrc.nist.gov/healthcare-testimony33000.htm

Katz, D. (2000, June). Elements of a comprehensive security solution. Retrieved October 4, 2001, from http://www.healthmgttech.com/archives/

Korpman, R. M.D. (2001). The third route to HIPAA compliance. *Health Management Technology,* 22(9), 38-40.

Medical Center Memorandum, (MCM) No. 00-16. (2002). *Statement of organizational ethics.* (NAVAHCS publication). Prescott, AZ: Author.

Medical Center Memorandum, (MCM) No. 0Q-07. (2002). *Disposal of sensitive material.* (NAVAHCS publication). Prescott, AZ: Author.

Medical Center Memorandum, (MCM) No. 0Q-12. (2002). *Informed consent.* (NAVAHCS publication). Prescott, AZ: Author.

Medical Center Memorandum, (MCM) No. 15-17. (2002). *Medical records.* (NAVAHCS publication). Prescott, AZ: Author.

Medical Center Memorandum, (MCM) No. 15-20. (2002). *The Privacy Act of 1974 (Release of information).* (NAVAHCS publication). Prescott, AZ: Author.

Medical Center Memorandum, (MCM) No. 15-26. (2002). *Automated information systems (AIS) security policy*. (NAVAHCS publication). Prescott, AZ: Author.

Mitchell, A. (2000, December 14). Cost impact of proposed privacy rules dramatically underestimated by federal government. Retrieved October 17,2001, from http://www.aha.org/info/releasedisplay.asp?passreleaseid=310

Morreim, E. (1995). Balancing act: The new medical ethics of medicine's new economics. Washington, DC: Georgetown University Press.

NAVAHCS. (1999). Data Backup Plan. Emergency mode operation plan addressing infrastructure*. ISSL Green Book.* (NAVAHCS publication). Prescott, AZ: Author.

NAVAHCS. (2000, March). VistA Contingency Plan Northern Arizona VA Health Care System Prescott, Arizona. (NAVAHCS publication). Prescott, AZ: Author.

Noble, S. (2001). For and against privacy regs. *Health Management Technology,* 22(9*)*, 2. Retrieved September 18, 2001, from http://healthmgttech.com/archives/

Nolin, C. (2001, August). Physicians, vendors and HIPAA compliance. Retrieved September 18, 2001, from http://healthmgttech.com/archives/

Office for Civil Rights. (2001). Standards for privacy of individually identifiable health information [45 CFR Parts 160 and 164]. Retrieved July 10, 2001, from http://www.hhs.gov/ocr/hipaa/

Office of Information HIPAA Coordinator. (2000). Overview of health insurance portability and accountability act of 1996 [Brochure]. Washington, DC: Author.

Office of the Assistant Secretary for Planning and Evaluation, DHHS. (2000, December 28). Standards for privacy of individually identifiable health information. Retrieved July 31, 2001. from http://www.hhs.gov/ocr/part1.html

Phoenix Health Systems. (2001). HIPAAdvisory: What's HIPAA? - A basic HIPAA primer. Retrieved August 29, 2001, from http://www.hipaadvisory.com/regs/HIPAAprimer1.htm

Presentation by the AHA to the national committee on vital and health statistics' (NCVHS): Hearing by the subcommittee on privacy and confidentiality – Panel on consent. (August 21, 2001). Washington, DC.

Putt, S. (2000, September 27). Overview of health insurance portability and accountability act of 1996. Retrieved August 29,2001, from http://vaww.va.gov/hipaa

QuadraMed. (2001, January). Hipaa-IQ executive summary. Retrieved September 27, 2001, from http://www.hipaa-iq.com/summary.htm

Roach, M. (2001). HIPAA compliance questions for business partner agreements. Retrieved September 18, 2001, from http://www.ahima.org/journal/features/feature.0102.1.htm

Secretary of Health and Human Services.(1997, September). Confidentiality of individually identifiable health information. Retrieved August 3, 2001, from http://aspe.os.dhhs.gov/admnsimp/pvcrec.htm

Shalala, Donna E. (1997, September 11). Confidentiality of individually identifiable health information. Retrieved August 30,2001, from http://aspe.os.dhhs.gov/admnsimp/pvcrec.htm

Stewart, S. (2001). Partnering with the private sector: Interview with Ken Clark on HIPAA. *CBI News - VHA Office of Compliance and Business Integrity,* 1(3), 5.

Taylor, D. (2001). Decoding HIPAA: A 6-point guide. *Outpatient Surgery Magazine,* 11(6), 24-31.

Thompson, T. (2001, April). Statement by HHS secretary Tommy G. Thompson regarding the patient privacy rule. Retrieved July 10, 2001, from http://www.hhs.gov/news/press/2001pres/20010412.html

Tirone, A. (2001, July). How HIPAA affects JCAHO accreditation. Ask The Experts – Joint Commission Perspectives.

U.S. Department of Health and Human Services Office of Civil Rights. (2001, July 6). Standards for privacy of individually identifiable health information (45 CFR Parts 160 and 164). Retrieved August 31, 2001, from http://www.hhs.gov/ocr

VHA Office of Information. (1999, November). HIPAA Impacts on VistA (initial). (VHA IO Technical Services, VDSI publication). Washington, DC: Author.

VHA Office of Information. (2000). Methodology for baseline assessments and gap analyses. Retrieved August 16, 2001, from http://vaww.va.gov/hipaa/HIPAA_workgroup.htm

VHA Office of Information. (2001, July 13). HIPAA Compliance Plan for Electronic Transactions and Privacy Standards. *Health Insurance and Accountability Act (HIPAA) Workgroup.* (VHA IO Technical Services, VDSI publication). Washington, DC: Author.

VHA Office of Information. (2001, August). OI top issues. Retrieved January 16 2002, from http://vaww.va.gov/vhacio/topten/currentten.cfm

VHA Office of information HIPAA Workgroup. (2000, September). Justification for VHA HIPAA Management Office. (VHA IO Technical Services, VDSI publication). Washington, DC: Author.

VHA Transition Paper. (2001,January). Health Insurance Portability and Accountability Act (HIPAA). VHA Office of Information, Washington, DC: Author.

VISN 18. (2002, January 9). VISN 18 Business Operations Executive Board. *Minutes from the VISN 18 Business Operations Executive Board Meeting.* Phoenix, AZ.

Walsh, D. (2001). I T Gatekeeper. *Military Medical Technology,* 5(4), 7-11.

Weber, B. (2001). Avoiding HIPAA hype: Preparing for HIPAA affordability. *Healthcare Financial Management,* (August*),* 1-3. Retrieved March 23, 2002, from www.findarticles.com/cf_0/m3257/8_55/78363250/pl/article

Wilson, K., & McPherson, C. (2002). It's 2002: How HIPAA-ready are you? *Health Management Technology,* 23(1), 14-20.

Zender, A. (2000). Next steps? First steps? Getting a grip on HIPAA security standards. Retrieved September 24, 2001, from http://www.ahima.org/journal/features/feature.0004.4html